US DEPARTMENT OF ENERGY

OFFICE OF SCIENCE

NATIONAL SECURITY SYSTEM

PROGRAM CYBER SECURITY PLAN

IMPLEMENTATION MANUAL

April 2007

CONTENTS

CHAPTER 1: INTRODUCTION 1

1.1 PURPOSE AND APPLICABILITY 1

1.2 TARGET AUDIENCE 1

1.3 RELATIONSHIP TO OTHER SECURITY CONTROL PUBLICATIONS 1

1.4 MANUAL ORGANIZATION AND STRUCTURE 2

CHAPTER TWO: SITE PROGRAM REQUIREMENTS 2

2.1 ORGANIZATIONAL RESPONSIBILITIES 3

2.2 NSS PROGRAM REQUIREMENTS 7

2.2.1 Site Review 8

2.2.2 Protection Requirements 9

2.2.3 Configuration Management 9

2.2.4 Training and Awareness 9

2.2.5 Information Marking 10

2.2.6 Storage Requirements 11

2.2.7 Visitor Access Requirements 11

2.2.8 Interconnected Systems 11

2.2.9 NSS Security Program Coordination 12

2.2.10 Incident Handling and Response 12

2.2.11 Clearing, Purging, and Destruction 13

2.2.12 System Security Plans 13

2.2.13 Certification and Accreditation 14

2.2.14 Metrics 14

CHAPTER THREE: DETERMINING RISK AND CONSEQUENCE OF LOSS 15

3.1 MANAGING RISK 16
3.2 SECURITY CATEGORIZATION 17
3.3 SELECTING AND TAILORING THE INITIAL CONTROLS 17
3.3.1 Scoping Guidance 18
3.3.2 Compensating Security Controls 18
CHAPTER FOUR: SECURITY CONTROL ORGANIZATION AND STRUCTURE 19
4.1 SECURITY CONTROL STRUCTURE 19
4.2 COMMON SECURITY CONTROLS 22
4.3 SYSTEM-SPECIFIC SECURITY CONTROLS 23
4.4 SECURITY CONTROLS FOR HOSTED SYSTEMS 23
4.5 APPLYING SECURITY CONTROLS TO SC SYSTEMS 24
APPENDIX I: REFERENCES I-1
APPENDIX II: GLOSSARY II-1
APPENDIX III: ACRONYMS III-1
APPENDIX IV: COMMON SECURITY CONTROLS IV-1
APPENDIX V: PERIODS PROCESSING SECURITY CONTROLS V-1
APPENDIX VI: ISOLATED NETWORK SECURITY CONTROLS VI-1
APPENDIX VII: NETWORKED SECURITY CONTROLS VII-1
APPENDIX VIII: PL 5-7 SECURITY CONTROLS VIII-1
APPENDIX IX: SUPPLEMENTAL CONTROLS FOR INTEGRITY AND AVAILABILITY IX-1
APPENDIX X: MAPPING TABLES X-1
APPENDIX XI: SECURITY PLAN TEMPLATES XI-1
APPENDIX XII: SAMPLE MOU/MOA XII-1
APPENDIX XIII: NSS MANUAL CONTROL COMPARISON XIII-1

CHAPTER 1: INTRODUCTION

This document outlines the Department of Energy (DOE) Office of Science (SC) implementation of DOE M 205.1-4, *National Security System (NSS) Manual*, dated 3/8/2007 and the SC Program Cyber Security Plan (PCSP). It describes the mandatory technical, operational and assurance controls required to secure National Security Systems housed and hosted at SC sites, and represents an approach to securing SC classified cyber assets based on compliance with Federal and DOE policy and the consequence of loss (CoL) for confidentiality, integrity, and availability and the sensitivity of the information based on classification level, category, and need-to-know. The requirements outlined within this document facilitate the implementation of appropriate controls for classified information that reflect the SC mission at the sites, as well as a rigorous defense in depth for classified information and information systems according to national laws and DOE policy.

1.1 PURPOSE AND APPLICABILITY

The purpose of this DOE SC NSS PCSP Implementation Manual ("Manual") is to provide SC sites with the required program, operational, technical and assurance controls for sites and information systems processing, storing, or transmitting classified information. The required controls apply to all SC sites and systems that house or host classified information.

1.2 TARGET AUDIENCE

This Manual is directed toward all SC Information System Security Managers (ISSMs), Information System Security Officers (ISSOs), and System Owners (SOs) at all SC sites that house or host classified information. It should also be used by DOE Designated Approving Authorities (DAAs) and auditors to validate the controls in place for the NSS under their purview.

1.3 RELATIONSHIP TO OTHER SECURITY CONTROL PUBLICATIONS

This Manual implements the requirements outlined in DOE M 205.1-4, *National Security System Manual*, dated 3/8/2007, DOE M 470.4-4, *Information Security*, and the SC PCSP. It is aligned with the National Industrial Security Program Operating Manual (NISPOM), the Federal Information Security Management Act of 2002 (FISMA), and with the National Institute of Standards and Technology (NIST) 800 Series Special Publications.

1.4 MANUAL ORGANIZATION AND STRUCTURE

This Manual is organized around the concept that there are "bundles" of controls that can be layered upon each other to provide the appropriate level of assurance required for the information being processed, as well as the configuration of the information system processing the information. It is structured as follows:

- Chapter Two provides the overall expectations for NSS program management at SC sites, including roles and responsibilities and SC site program requirements.
- Chapter Three provides the process to determine the CoL and risk categorization for SC NSS.
- Chapter Four outlines the security control organization and structure, and provides an example of how the control layering concept works for SC NSS systems.
- Supporting appendices provide:

I. References

II. Glossary

III. Acronyms

IV. NSS Common Security Controls

V. NSS Periods Processing System Controls

VI. NSS Isolated Network System Controls

VII. NSS Networked System Controls

VIII. NSS Protection Level (PL) 5-7 Security Controls

IX. Supplemental Controls for Integrity and Availability

X. Mapping Tables relating the security controls in this document to other standards and control sets

XI. Security Plan Template

XII. Sample Memorandum of Understanding/Memorandum of Agreement (MOU/MOA)

XIII. NSS MANUAL CONTROL COMPARISON

CHAPTER TWO: SITE PROGRAM REQUIREMENTS

This chapter outlines the requirements for implementing an effective NSS program at SC sites that considers the unique threats to, and mission of the site and integrates these concerns with site operations to develop a cyber defense. It includes a program implementation that identifies, evaluates, and integrates the impact of information loss, system vulnerabilities, data custodian protection requirements, cost of protective measures, and mission requirements. SC NSS program management assures compliance with Federal and DOE policy, and system operation where the remaining risk (residual risk) is accepted and oversight is initiated to ensure that the level of residual risk is managed throughout the information system's life cycle.

2.1 ORGANIZATIONAL RESPONSIBILITIES

The following are the primary roles and responsibilities with regard to National Security Systems at SC sites. Other responsibilities are outlined in DOE M 205.1-4, *National Security System Manual*, dated 3/8/2007 and the SC PCSP.

- Designated Approving Authority (DAA) –The Designated Approving Authority (DAA) is a senior management official or executive possessing the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals. The DAA has inherent U.S. government authority and, as such, must be a government employee. Within SC, the Site Office Manager or the Operations Office Manager where a Site Officer Manager does not exist is the DAA for their laboratory and their own organization and the Science Information Officer (SIO) is the DAA for SC Headquarters.
  - Serves as accrediting authority for each DOE and covered contractor NSS with operational boundaries fully contained under his/her jurisdiction.
  - Ensures that knowledgeable technical advisors are available to assist in and support the risk acceptance decision.
  - Ensures that this Manual is implemented for each NSS under his/her jurisdiction, that each system is accredited or reaccredited every 3 years unless a security-significant change occurs, and that the accreditation or reaccreditation is documented.
  - Ensures that the accreditation of each system under his/her jurisdiction is withdrawn, and that the system is properly sanitized when the system no longer processes classified information or when changes occur that might affect accreditation.
  - Reports any changes in ISSM appointments to the SC SIO.

- Information System Security Manager (ISSM) – The ISSM at a Federal Site is appointed by the DAA. The ISSM at an SC Contractor site is nominated by the Laboratory Director and appointed by the DAA to be responsible for implementation of the site NSS Security Program.
  - Establishes, documents, implements, and monitors the NSS Security Program for the site and ensures site compliance with Federal and DOE requirements for NSS.
  - Ensures the development of procedures for use in the site NSS Security Program.
  - Identifies and documents unique threats to information systems within the Master Plan.
  - Ensures the development, documentation, and presentation of NSS security education, awareness, and training activities for site management, information security personnel, data custodians, users, and escorts in NSS operational areas.
  - Coordinates the following:
    - Integration of the site NSS Security Program with the other site programs, as appropriate, such as Classified Matter Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Transmission Systems, TEMPEST, and Materials Control and Accountability;
    - Development of a site self-assessment program for the NSS Security Program; and performing self-assessments of the effectiveness of the site's NSS controls.
  - Ensures the development of site procedures to meet all protection measures outlined in the NSS Security Plan (SP).
  - Reviews and approves System Security Plans (SSPs), certification test plans, and certification test results.
  - Determines, using guidance from the data custodian(s), the appropriate levels of concern for confidentiality, integrity, and availability for each information system that processes classified information.
  - Recommends to the DAA, in writing, approval or disapproval of the SP test results and the certification statement.
  - Ensures that the DAA is notified when a system no longer processes classified information, or when changes occur that might affect accreditation.

- Participates in DOE-sponsored NSS security training within 1 year of his/her appointment, and participates in continuing education at least annually thereafter.

- Ensures that personnel are trained on the information system's prescribed security restrictions and safeguards before they are initially allowed to access a system.

❖ Information Systems Security Officer (ISSO)

The ISSO is appointed in writing by the ISSM, or the System Owner with approval of the ISSM.

- Ensures implementation of security measures for each classified information system for which he/she is responsible.

- Identifies and documents any unique threats to NSS for which he/she is the ISSO, and forwards them to the ISSM.

- If so directed by the DAA or ISSM and/or if an identified unique local threat exists, performs a risk assessment to determine if additional countermeasures beyond those identified in this Manual are required.

- Develops and implements a certification test plan for each classified information system for which he/she is the ISSO, as required by this Manual and the DAA.

- Prepares, maintains, and implements an SP that accurately reflects the installation of protection measures for each NSS for which he/she is responsible.

- Maintains the record copy of the SP and related documentation for each classified information system for which he/she is the ISSO.

- Notifies the ISSM when a system no longer processes classified information, or when changes occur that might affect accreditation.

- Ensures the following:

  - That the sensitivity level of the information is determined prior to use on the NSS and that the proper security measures are implemented to protect this information;

  - That unauthorized personnel are not granted use of, or access to, an NSS; and

  - That formal access controls are implemented for each NSS.

- Documents any special protection requirements identified by the data custodians and the protection measures implemented to fulfill these requirements for the

information contained in the classified information system. *Note: An ISSO may not also be the System Owner/Data Custodian for the system.*

- Ensures that confidentiality, integrity, and availability levels of concern are determined for each classified information system for which he/she is responsible.
- Implements site procedures to meet all protection measures outlined in the NSS SP.
- Requires that each classified information system user signs an acknowledgment of responsibility (Code of Conduct) for protecting NSS and classified information.
- Reviews and approve system-level SPs, certification test plans, and certification test results.
- Ensures that users are properly trained in system security by identifying classified information systems security training needs (including system-specific training) and personnel who need to attend system security training programs.
- Conducts ongoing security reviews and tests of NSS to periodically verify that security features and operating controls are functional and effective.
- Evaluates proposed changes or additions to the NSS and advises the ISSM of their security relevance.
- Participates in DOE -sponsored NSS security training within 1 year of his/her appointment, and relevant continuing education at least annually thereafter.

❖ NSS System Owner/Data Custodian

- Determines and declares the sensitivity level of information prior to the information being processed, stored, transferred, or accessed on the classified information system.
- Advises the ISSO of any special protection requirements for information to be processed on the classified information system. *Note: A System Owner/Data Custodian may not be also be the ISSO for the system.*
- Determines and documents the data and application(s) that are essential to fulfill the site mission, and ensures that requirements for contingencies are determined, implemented, and tested.

❖ System Administrator

- Configures the information system to conform with all requirements for NSS.
- Acknowledge, in writing, their responsibilities (Code of Conduct) for protecting classified information systems and classified information.
- Are accountable for their actions on NSS.
- Participate in training on information system security before accessing an NSS. Participates in an ongoing security education, training, and awareness program at least annually thereafter.

❖ NSS Users

- Comply with the NSS Security Program requirements.
- Are aware of and knowledgeable about their responsibilities in regard to NSS security.
- Are accountable for their actions on NSS.
- Ensure that any authentication mechanisms (including passwords) issued for the control of their access to NSS are not shared and are protected at the highest classification level and most restrictive classification category of information to which they permit access.
- Acknowledge, in writing, their responsibilities (Code of Conduct) for protecting classified information systems and classified information.
- Ensures that information that they create and process is on systems accredited at a level sufficient to protect the information.
- Participate in training on the information system's prescribed security restrictions and safeguards before being granted initial access to a system. Participate in an ongoing security education, training, and awareness program at least annually thereafter.

2.2 NSS PROGRAM REQUIREMENTS

SC sites are responsible for assuring that cyber security controls relevant to classified systems continue to work as intended, that the trust level of classified systems is maintained, and that all changes to the cyber security environment are properly recorded and analyzed for impact to the organization and its mission. Each SC site must establish, document, implement, and monitor the NSS Security Program for the site, and ensure site compliance with Federal and DOE requirements for NSS. The NSS Security

Program is documented within the site Classified Cyber Security Program Plan ("Master Plan") and associated procedures, which include:

- Site review
- Protection requirements
- Configuration management
- Awareness and training requirements
- Information marking requirements
- Storage requirements
- Visitor access requirements
- Interconnected systems
- Program coordination
- Incident handling and response requirements
- Clearing, purging, and destruction requirements
- System Security Plans
- Certification and Accreditation (C&A) requirements
- Metrics

The Master Plan should be aligned with this Manual, the SC PCSP, and all applicable Federal and DOE requirements.

2.2.1 SITE REVIEW

Each SC site must perform an annual assessment to determine the unique threats and risk to the site, and the effectiveness of the cyber security protection in place. This review is supplemental to the DOE-wide Threat and Risk Statement; the Site Visit process; and reviews conducted by the DOE Cognizant Security Authority, the Office of Assurance, Office of the Inspector General; or other audits which may be scheduled.

Site reviews must include an assessment of both programmatic and technical elements to verify that the required controls are in place and functioning as intended. It should demonstrate compliance with the SC PCSP, this Manual, and with all applicable Federal laws and DOE requirements. The output of the review should include a gap analysis that outlines any programmatic and technical shortcomings found and planned

remediation. The gaps should be reported as site Plans of Action and Milestones (POA&M), and closed within one year.

The threat and risk analysis is used to determine the level of protection required for the information processed at the site. The results of the site risk assessment must be documented and used to augment, as needed, the NSS protection profiles to be applied to classified information systems at the site. This analysis must be reviewed and updated by the ISSM at least annually.

2.2.2 PROTECTION REQUIREMENTS

All SC sites must protect classified systems and information, at a minimum, as stated in the Common Controls section of this Manual and documented in the Master Plan. Classified systems and information must be protected at the highest level of sensitivity contained in the document and system. Controls listed for each PL are mandatory for all systems within that PL. If additional controls are required due to a higher risk categorization or consequence of loss (CoL), they must be documented within an approved system SP.

All personnel must meet all requirements outlined in DOE M 470.4-4, *Information Security* and DOE M 470.4-5, *Personnel Security* prior to being granted access to classified systems and/or information.

2.2.3 CONFIGURATION MANAGEMENT

All NSS systems must be under configuration control and managed according to the controls outlined in this Manual and documented in the Master Plan. Security-significant changes to the documented configuration of a system immediately nullify its current Authority To Operate. “Security significant changes” are defined at the site level in the Master Plan, and approved by the DAA. The DAA must review all proposed modifications to information systems to determine if the modifications will impact the protections and accreditation of the information systems. All changes must be documented, and the system must be re-accredited by the ISSM and DAA before transaction processing may resume.

2.2.4 TRAINING AND AWARENESS

All SC sites are required to provide a comprehensive training program and awareness briefings and activities for site NSS program management personnel, information security personnel, system administrators, data custodians, users, and escorts in NSS operational areas. Training must be completed prior to being issued authentication credentials for system access, and refreshed yearly thereafter. All users must sign an

acknowledgement signifying their understanding of their responsibilities (Code of Conduct) for protecting classified information systems and classified information.

The ISSM and ISSO must participate in DOE-sponsored training within one year of their appointment. All personnel who hold a security-relevant position (ISSM, ISSO, and system administrators) must attend cyber security training that is relevant to their job at least annually. The ISSM must document procedures for maintaining a training plan and record for all personnel in security-relevant positions.

The site training program must meet all requirements outlined in DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, Sections J and K.

2.2.5 INFORMATION MARKING

Classified information and systems must be marked at the highest level of sensitivity contained in the document and system and in accordance with DOE M 470.4-4, *Information Security*.

- Hardware Components – Procedures must be implemented to ensure that components of an information system, including input/output devices, terminals, stand-alone microprocessors, or word processors used as terminals, bear a conspicuous, external label that states the highest classification level and most restrictive classification category of the information accessible to the component in the information system. This labeling may be accomplished using permanent markings on the component, a sign permanently fixed to a terminal, or labels generated by the information system and displayed on the screen.

- Hard-Copy Output – Hard-copy output includes paper, fiche, film, and other printed media. The classification level of the output must be marked on all hardcopy output that is retained in, or distributed from, the facility. The marking must be automatically generated on the output by the system. Before release outside the activity an appropriate classification review must be conducted, or the information must be generated by a tested program verified to produce consistent results and which has been approved by the DAA. Such programs will be tested on a periodic basis to ensure continuing performance. Once hard copy has been reviewed by an authorized classifier, it must be marked in accordance with DOE M 470.4-4, *Information Security*.

- Removable Media – Procedures must be implemented to ensure that personnel handling removable media apply visible, human-readable, external markings to the media. Removable media must be marked with the highest classification level of the information contained on the system, or if the information on the media has been generated by a tested program or methodology verified to produce consistent results

and which has been approved by the DAA. Classified Removable Electronic Media (CREM) and Accountable CREM (ACREM) must be handled, stored, documented, and protected as outlined in DOE M 470.4-4, *Information Security*.

- Unclassified Media – In facilities where some of the information systems are operated as classified and some are dedicated to unclassified operation, removable unclassified media must be uniquely marked to prevent them from being mixed with classified media. Unmarked blank media must not be stored in an area used for classified processing. Except in periods processing environments, media should not be compatible with both unclassified and classified systems within the same certification boundary.

2.2.6 STORAGE REQUIREMENTS

All classified information (electronic and hard copy) stored on site must be protected as outlined in the controls stated in this Manual, and stored in accordance with DOE M 470.4-4, *Information Security* and in DOE M 470.4-2, *Physical Protection.*

2.2.7 VISITOR ACCESS REQUIREMENTS

Strict physical access control procedures must be in place at all sites where classified processing, storage, or transmission takes place. All users must be trained in the requirements for allowing visitors into areas where this information resides. Visitor control requirements are outlined in DOE M 470.4-4, *Information Security,* DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*, and DOE O 142.1, *Classified Visits Involving Foreign Nationals*.

2.2.8 INTERCONNECTED SYSTEMS

Sites that manage NSS that contain, process, or transmit classified information to other entities must develop, document, and implement interconnection policies and procedures consistent with TMR 5, *Interconnected Systems Management,* the following criteria, and be commensurate with the level of security required for the organization's environment and specific needs. The documentation must include:

- The purpose of the interconnection, such as types of services to be provided through the interface, types of information allowed to flow over the interface, and method of data exchange.
- Baseline configuration of the interface, such as identification of hardware specifications, identification of protocols, identification of data formats, identification of allowed services, and identification of systems authorized to communicate over the interface by network address/Domain Name Service name.

- Identification of methods to meet the security requirements of the interconnected systems and/or adjudicate security implementation differences (e.g. clearances information protection methods, etc.) between interconnected systems. A Memorandum of Understanding/Memorandum of Agreement (MOU/MOA) must be signed by all entities. The MOU/MOA is a written agreement of cooperation between organizations defining the roles and responsibilities of each organization in relation to the other with respect to security issues over which the organizations have concurrent jurisdiction. The purpose of the MOU/MOA is to assure that the security posture of either organization is not degraded by changes to the security controls implemented for either network. A sample MOU/MOA is provided in Appendix XII. The MOU/MOA identifies the specific responsibilities and acceptance of residual risk between the interconnected parties as follows:
  - Responsibilities and processes for mutual configuration management and change notification for the interface.
  - Responsibilities and processes for mutual maintenance and operation of the interface.
  - Responsibilities, processes, and methods for mutual incident response and reporting to include attacks and interface component failures.
  - Responsibilities and processes for establishing cross-domain accounts.
  - Mutual acceptance of residual risk.

The interconnection must be approved as part of the system certification and accreditation by the cognizant DAA for each interconnected party.

Classified facsimile machines, printers, and copiers and their interconnections with NSS or other entities must be set up to comply with all requirements of DOE O 470.4-4, *Information Security*, and DOE M 205.1-3, *Telecommunications Security Manual*. These devices must be certified and accredited as part of the NSS Security Program prior to being placed in use.

2.2.9 NSS SECURITY PROGRAM COORDINATION

The NSS Security Program at each site must ensure that the program is coordinated with other site programs governing classified information, as appropriate, such as Information Security, Personnel Security, Physical Security, Communications Security, Protected Transmission Systems, Telecommunication Security, TEMPEST, and Materials Control and Accountability.

2.2.10 INCIDENT HANDLING AND RESPONSE

Sites are required to maintain a rigorous Cyber Incident Response program for classified information, which includes the establishment of a Cyber Incident Response Team (CIRT) that is trained in proper incident handling procedures. The program must include all required elements outlined in Attachment 2, Part II, Section N, Chapter II, *Incidents of Security Concern Involving Compromise or Potential Compromise of Classified Information* of DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.

2.2.11 CLEARING, PURGING, AND DESTRUCTION

All SC sites must develop, document, and implement processes for the clearing, purging, and destruction of classified media, storage devices, and other hardware utilizing the applicable criteria in CS-11, *Media Clearing, Purging and Destruction Guidance* and commensurate with the level of security required for the organization's environment and specific needs.

The requirements for removing information from storage media, memory devices, and related hardware are to be reviewed with all users on a regular basis. Personnel performing or verifying the clearing, purging, or destruction of storage media, memory devices, and other hardware are to be trained in equipment/tool operation, approved techniques, and procedures.

2.2.12 SYSTEM SECURITY PLANS

All systems storing, processing, or transmitting classified information must be supported by an approved Security Plan. The technical, operational, and assurance controls that comprise the overarching set of security controls for all systems are documented in the Security Plan, including any additional implementation information for the controls. Any additional controls resulting from adjustments identified during the risk management process must also be included in the Security Plan.

Security controls that are common for multiple systems must be documented in at least one approved Master SP associated with an accredited information system. The certification and accreditation of that system will verify that the controls have been correctly implemented and are effective. New systems that are added to the site following the approval of the Master Plan require DAA-approved testing to validate the correct implementation of the control(s) in the new information system. The Master Plan will specify the information required for new systems which are accredited under the plan.

An Individual System Security Plan, which is appended to the Master SP, contains the individual information system identification and categorization, points of contact, system characterization (system component and software inventory, configuration

management documentation, locations, testing and inspection records, etc.). If an individual system's configuration varies from an approved Master Plan, the system must be certified and accredited separately.

All Security Plans must be reviewed annually by the ISSM and accredited by the DAA every three years, or when a security significant change occurs. Individual System Security Plans must be reviewed and if required updated annually, or when a security significant change occurs.

2.2.13 CERTIFICATION AND ACCREDITATION

All NSS systems must be properly certified and accredited prior to being placed in use in accordance with the DOE NSS Manual. The formal C&A occurs after the required protection measures have been implemented and any required protection documentation has been approved. Certification validates that the protection measures described in the SSP have been implemented on the system, and that the protection measures are functioning properly. Accreditation is the approval by the DAA for the system to process classified information.

For a system or group of systems that involve multiple DAAs (e.g., cross-certification with other agencies), the DAA for the system owner is considered the primary DAA, and the SC site DAA functions as a "landlord" for the data or connection at the DOE site. The security official under the primary DAA prepares the C&A documentation, which will include specific roles and responsibilities for each facility included in the certification. The system is first certified locally, and then submitted to the DAA for the SC site for an Authority to Operate through an MOU/MOA.

2.2.14 METRICS

In order to meet reporting requirements for FISMA and SC, metrics documentation and reporting is required for all sites. SC may also require site reporting for ad hoc data calls in order to maintain an accurate representation and reporting of the status of the NSS program to meet developing federal, DOE, or SC requirements as they arise.

2.2.14.1 OFFICE OF SCIENCE METRICS

SC requires quarterly reporting of FISMA metrics.

2.2.14.2 SITE CYBER SECURITY METRICS

Individual sites are required to maintain metrics information and reporting as outlined in the control sets, at a minimum, for the following information:

- Incident occurrences and reports

- Vulnerability testing and mitigation activities

2.2.14.3 STATUS REPORTING AND DOCUMENTATION

Due to the ever-changing cyber security climate, federal, DOE, or SC entities may require ad hoc data call reporting to gauge the current status of NSS security or elements therein. To facilitate this process, all reporting and documentation requirements outlined within this Manual and the appended control sets must be met.

2.2.14.4 PLAN OF ACTIONS AND MILESTONES

All SC sites are required to maintain a current Plan of Action and Milestone (POA&M) list that contains:

- Unresolved findings from audits and assessments
- Planned improvements affecting the cyber posture of the site NSS Security Program

POA&Ms are to be closed within twelve months. Longer-term POA&Ms, status, and plan for closure must be reported within the quarterly FISMA reports to SC. Closed POA&Ms remain on the report for one year from closure.

CHAPTER THREE: DETERMINING RISK AND CONSEQUENCE OF LOSS

This chapter describes the process by which risk and consequence of loss (CoL) for NSS information is analyzed and selected. NSS information is grouped based on sensitivity (classification level). The following describes the information groups, also known as the Protection Level (PL), used by the DOE in increasing order of sensitivity (Top Secret Restricted Data considered the most sensitive). A PL contains all information types that require similar protection or are similar in content or use. The information groups are:

- PL-1: Confidential/Secret (C/S) – Information that is classified as Confidential National Security Information, Confidential Formerly Restricted Data, Confidential Restricted Data, Secret National Security Information, or Secret Formerly Restricted Data and does not contain any nuclear weapons data.
- PL-2: Secret Restricted Data (SRD) – Information that is classified Secret Restricted Data and does not contain any nuclear weapons data.
- PL:-3: Confidential Restricted Data, Sigmas 1 through 13 (CRD1-13) – Information that is classified as Confidential and identified as Restricted Data, Formerly Restricted Data, or is related to nuclear weapons, contains information that falls in at

least one of the sigma categories 1 through 13 as described in DOE O 5610.2, *Control of Weapon Data*, and successors.

- PL-4: Secret Restricted Data, Sigmas 1 through 13, 15 and 20 (SRD1-13, 15, 20) – Information that is classified as Secret and identified as Restricted Data and is related to nuclear weapons and contains information that falls within at least one of the sigma categories 1 through 13, 15 and 20 as described in DOE O 5610.2, *Control of Weapon Data*, and successors.

- PL-5: Secret Restricted Data, Sigma 14 (SRD14) – Information that is classified as Secret and identified as Restricted Data or is related to nuclear weapons and contains information that falls within the Sigma 14 category, as described in DOE O 5610.2, *Control of Weapon Data*, DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Design*, and DOE O 457.1, *Nuclear Counterterrorism*, respectively and their successors.

- PL-6: Top Secret (TS) – Information that is classified as Top Secret National Security Information or Top Secret Formerly Restricted Data.

- PL-7: Top Secret Restricted Data (TSRD) – Nuclear Weapons information that is classified Top Secret.

3.1 MANAGING RISK

The selection and specification of security controls for an information system requires the management of the risk to the organization or to the individuals associated with the operation of the information system. Risk categorization, combined with the system CoL determination, provides an effective framework for selecting the appropriate security controls for an NSS. The following activities (from the NIST *Risk Management Framework*) are to be performed as part of the risk management process for managing NSS systems:

- ***Categorize*** the information system and the information resident within that system based on a Federal Information Processing Standard (FIPS) 199 impact analysis.

- ***Select*** an initial set of security controls (baseline) for the information system based on the security categorization (classification) and the minimum security requirements defined in this Manual to obtain the control set used as the starting point for the assessment of risk associated with the use of the system.

- ***Supplement*** the initial set of tailored security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.

- ***Document*** the agreed-upon set of security controls in the system security plan including the organization's rationale for any refinements or adjustments to the initial set of controls.
- ***Implement*** the security controls in the information system.
- ***Assess*** the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- ***Authorize*** information system operation based upon a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system, following the authorization to operate and acceptance of residual risk by the DAA.
- ***Monitor*** and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis.

3.2 SECURITY CATEGORIZATION

Each system must be categorized based on the highest PL, or level of classification, for the information processed, stored, or transmitted on the system. The baseline controls must then be analyzed in light of any decision by Senior DOE Management, SC, the ISSM, or the information system owner to increase the CoL (e.g., due to the identification of a threat not identified in the DOE or Site Threat Statement, and/or identification of a standard practice not identified in the control set for a protection level).

3.3 SELECTING AND TAILORING THE INITIAL CONTROLS

Once the overall impact level of the information system is determined, an initial set of security controls can be selected from the corresponding control sets listed in Chapter Four based upon the system type (single-user standalone, multi-user, interconnected system, etc.). Sites have the flexibility to tailor the security controls in accordance with the CoL determination. Tailoring activities include the application of appropriate scoping guidance to the initial baseline and the specification of additional security controls, if needed. To achieve a compliant, risk-based approach to providing adequate information security organization-wide, security control baseline tailoring activities should be coordinated with, and approved by, appropriate organizational officials (e.g.,

ISSM, DAA). Tailoring decisions should be documented in the security plan for the information system.

3.3.1 SCOPING GUIDANCE

There are several considerations, described below, that can potentially impact how the baseline security controls are applied by the ISSO and/or SO:

- Common security control-related considerations – Security controls designated as common controls (applicable to all NSS systems) are, in most cases, managed by the ISSM as part of the NSS Security Program at the site, and may greatly affect the responsibilities of individual system owners with regard to the implementation of individual controls for the system(s) under their purview. Every control in the common control set must be fully addressed either by the site's overarching security plan or the system owner.

- Operational/environmental-related considerations – Security controls that are dependent on the nature of the operational environment are applicable only if the information system is employed in an environment necessitating the controls. For example, certain physical security controls may not be applicable to diskless terminals.

- Physical Infrastructure-related considerations – Security controls that refer to organizational facilities (e.g., physical controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) are applicable only to those sections of the facilities that directly provide protection to information systems or information in any form (e.g. assets such as servers, networking nodes, boundary protection devices, and communications equipment, as well as physical storage for hardcopy documents).

- Technology-related considerations – Security controls that refer to specific technologies (e.g., cryptography) are applicable only if those technologies are employed or are required to be employed within the information system.

3.3.2 COMPENSATING SECURITY CONTROLS

System Owners and/or ISSMs may find it necessary, on occasion, to specify and employ compensating security controls. A compensating security control is an assurance, operational, or technical control (i.e., safeguard or countermeasure) employed in lieu of a recommended security control that provides equivalent or comparable protection for an information system. A compensating control for an information system may be employed only if the SP provides a complete and convincing rationale for how the compensating control provides an equivalent security capability or level of protection

for the information system; why the related baseline security control could not be employed; and if the ISSM assesses and the DAA formally accepts the risk associated with employing the compensating control in the information system. The use of compensating security controls shall be documented in the security plan for the system and approved by the DAA.

CHAPTER FOUR: SECURITY CONTROL ORGANIZATION AND STRUCTURE

This chapter presents the fundamental concepts associated with security control selection and specification including: the structure of security controls and the organization of the controls in the control catalog; the identification and use of common security controls; system-specific security controls; hosting NSS information; and the layering schema for the control sets presented in Appendices IV-VIII.

4.1 SECURITY CONTROL STRUCTURE

The NSS manual provided three tables that describe the CoL for confidentiality, integrity and availability. [1]These tables divide the CoL into categories ranging from "very low" to "very high". The CoL from all the tables were analyzed by DOE and results of the analysis is represented in the table below.

TABLE 1. CONSEQUENCE OF LOSS OF CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

Protection Level	Information Group			Loss of Confidentiality	Loss of Integrity	Loss of Availability
PL-1	Confidential/Secret			Medium	Low	Very Low
PL-2	Secret Restricted			Medium	Low	Very Low
PL-3	Confidential Restricted Data	Sigma[2]	1, 2, 3, 4, 5, 9, 10, 11, 12, and 13	High	Low	Very Low
PL-4	Secret Restricted Data	Sigma	1, 2, 3, 4, 5, 9, 10, 11, 12, and 13	High	Low	Very Low
PL-5	Secret Restricted Data	Sigma	14, 15, and 20	Very High	Low	Very Low

[1] See pages I-3 to I-5 of NSS manual

[2] Sigmas 6, 7, and 8 are not currently in use.

Protection Level	Information Group	Loss of Confidentiality	Loss of Integrity	Loss of Availability
PL-6	Top Secret	Very High	Low	Very Low
PL-7	Top Secret Restricted Data	Very High	Low	Very Low

The sole differentiator for the protection level in the table is loss of confidentiality. The protection levels can thus be combined into three groups with no loss of rigor for the defense in depth required for National Security systems. The consolidated protection levels utilized by SC are represented in the table below.

TABLE 2. SIMPLIFIED COL OF CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

Protection Level	Information Group			Loss of Confidentiality	Loss of Integrity	Loss of Availability
PL-1-2	Confidential/Secret Secret Restricted			Medium	Low	Low
PL-3-4	Confidential Restricted Data / Secret Restricted Data	Sigma	1, 2, 3, 4, 5, 9, 10, 11, 12, and 13	High	Low	Low
PL-5-7	Secret Restricted Data Top Secret Top Secret Restricted Data	Sigma	14, 15, and 20	Very High	Low	Low

Availability and integrity of information is a discriminator in determining the controls that must be applied to properly protect classified information. SC requires that additional controls from NIST be applied as needed to assure that information which has a higher consequence of loss due to integrity or availability concerns is adequately protected. All sites must assess the CoL for integrity and availability and apply the supplemental controls outlined in Appendix IX.

The NSS manual contains three classes of controls – technical, operational and assurance. Technical controls are intended to be implemented within the information system through means employing software, hardware, or firmware. Operational controls are implemented within the environment in which the information system resides through processes and procedures. Assurance controls are implemented through actions taken by system owners (developers and implementers) of security controls to use state-of-the-practice design, development, and implementation techniques and

methods; and actions taken by security control certifiers during the C&A process to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

A two-character identifier is assigned to uniquely identify each control family. Table 3 summarizes the classes and families in the National System Security Manual.

TABLE 3. NATIONAL SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

IDENTIFIER	FAMILY	CLASS
AU	Security Audit Control	Technical
CO	Communication Control	Technical
CS	Cryptographic Support Control	Technical
DP	User Data Protection Control	Technical
IA	Identification and Authentication Control	Technical
MT	Security Management Control	Technical
PT	Protection of Information system Security Control	Technical
RU	Resource Utilization Control	Technical
SA	System Access Control	Technical
TP	Trusted Path Control	Technical
EN	Operational Control	Operational
CM	Configuration Management Control	Assurance
DO	Delivery and Operations control	Assurance
DV	Development Control	Assurance
GD	Guidance Documents Control	Assurance
LC	Life-Cycle support Control	Assurance
TE	Test Control	Assurance
VA	Vulnerability Assessment Control	Assurance

NIST 800-53 Rev. 1, *Recommended Security Controls for Federal Information Systems* contains 17 families of controls used to protect unclassified information, and are used to determine which controls to incorporate to protect information that has a CoL above "low" for integrity and availability. The above control families for NSS information have been mapped to the NIST control families, and are outlined in Appendix X, *Mapping Tables*.

The controls in the NSS manual do not protect information in hard copy form, which is still considered a cyber security responsibility, as hard copy information is generated through the NSS.

Appendices IV-IX provide detailed descriptions of each control. The following taxonomy is used to describe each control.

- Two-letter designation – identifies the family of the control. There are 18 families of controls for national security systems. There are three classes of controls: Technical, Operational, and Assurance.
- Dash number – identifies the number of the control within the family
- Parenthetical number – identifies enhancements to the control which are required for higher protection levels.[3]
- If supplemental NIST controls are incorporated, the NIST two-character identifier and number will be used along with an asterisk to indicate the control is from NIST.

  For example: A high-level session termination control from NIST is presented as *AC-12(1).

4.2 COMMON SECURITY CONTROLS

[3] The control enhancements section provides statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. In both cases, the control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to a basic control's functionality based on the results of a risk assessment. Control enhancements are numbered sequentially within each control so that the enhancements can be easily identified when selected to supplement the basic control. In the example above, if all three control enhancements are selected, the control designation subsequently becomes AU-2 (1) (2) (3). The numerical designation of a security control enhancement is used only to identify a particular enhancement within the control structure. The designation is neither indicative of the relative strength of the control enhancement nor assumes any hierarchical relationship among enhancements. In the above example, enhancement (3) is used before (1) and (2) since that enhancement is appropriate at a lower level than the other two. This type of situation arises from the decision to enhance control stability in the face of change by not renumbering existing enhancements when new ones are added or when decision about placement within baseline changes.

There is a baseline set of security controls required to protect all SC NSS (i.e., configuration management, delivery and operations, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls). These common controls are identified in Appendix IV. The common controls apply to all configurations within the Office of Science Laboratories and site offices, and all are required for the secure operation of all NSS systems.

4.3 SYSTEM-SPECIFIC SECURITY CONTROLS

System specific security controls are dependent on the system functionality, configuration, and the protection level of the system. The following appendices contain the required system-specific controls for national security systems used within the Office of Science.

Appendix	Configuration	Protection level
IV	Common Controls/Single-User Standalone Systems	PL 1-4
V	Standalone Periods Processing Systems	PL 1-4
VI	Isolated Network System	PL 1-4
VII	Networked Systems	PL 1-4
VIII	All Systems	PL 5-7
IX	Supplemental Controls for Integrity and Availability	All

The ISSM should coordinate with the ISSOs and System Owners (SOs) responsible for the development and implementation of the designated security controls to ensure that the required controls are put into place, are assessed as required, and the assessment results are documented to support the security accreditation process.

4.4 SECURITY CONTROLS FOR HOSTED SYSTEMS

Some SC sites host national security systems for other organizations. It is the responsibility of the hosting site to require an ATO and MOU/MOA from the providing organization showing the requisite security controls are applied and operational, and do not present additional vulnerabilities to the infrastructure of the hosting facility.

The DAA must require that an appropriate chain of trust be established with the provider organization. This trust relationship and other rules of engagement are contained in the MOU/MOA between the organizations, and must be mutually assured.

4.5 APPLYING SECURITY CONTROLS TO SC SYSTEMS

The structure of the control sets in Appendices IV-VIII are designed to be layered according to the system type and/or PL. The control sets are:

- Common Controls – apply to all systems regardless of PL or network connectivity, including single-user standalone systems.
- Standalone Periods Processing Controls – apply to systems that operate in standalone (non-networked) environments and have either users with varying need-to-know or with information that has more than one PL.
- Isolated Network Controls – apply to systems which are networked together but not connected to any outside network (e.g., Local Area Network or diskless operations).
- Networked Controls – apply to systems or groups of systems which share at least one interface with an outside entity (e.g., Wide Area Network operations).
- PL 5-7 Controls – apply to all systems with a Protection Level of 5 or higher.
- Supplemental Controls for Integrity and Availability – apply to systems with a CoL that is higher than "Low" for Integrity and/or Availability.

The layering occurs as functionality is enhanced and/or PL becomes higher. For example, all systems must apply all controls in the Common Control set. If the system(s) are networked locally, the Common Control set *plus* the Periods Processing Control set (where applicable) *plus* the Isolated Network Control set must be applied. The table below outlines which control sets are required under this layering schema:

TABLE 4: CONTROL SET LAYERING

System	Control Set(s)
All	Common Controls
Standalone Periods Processing	Common Controls Periods Processing Controls
Isolated Network	Common Controls Periods Processing Controls (where applicable) Isolated Network Controls
Networked	Common Controls Periods Processing Controls Isolated Network Controls Networked Controls
PL 5-7	Common Controls Periods Processing Controls

System	Control Set(s)
	Isolated Network Controls Networked Controls PL 5-7 Controls

In addition to functionality, both the user's need-to-know and the class(es) of information contained within the system must be taken into consideration when applying a control set to a system or group of systems. Additional controls outside of a specific control set may be required in order to properly protect the system and data, and should be applied and documented in the SSP. Also, if the CoL for a system has been determined to be higher than "Low" for Integrity or Availability, the *Supplemental Controls for Integrity and Availability* outlined in Appendix IX must be applied and documented in the SP.

APPENDIX I: REFERENCES

CS-11, *Media Clearing, Purging and Destruction Guidance*, 11

DOE M 205.1-3, *Telecommunications Security Manual*, 11

DOE M 205.1-4, *National Security System (NSS) Manual*, 1

DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Design*, 14, 3

DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8, 11

DOE M 470.4-2, *Physical Protection*, 9

DOE M 470.4-4, *Information Security*, 1

DOE M 470.4-5, *Personnel Security*, 8

DOE O 142.1, *Classified Visits Involving Foreign Nationals*, 10

DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*, 10

DOE O 457.1, *Nuclear Counterterrorism*, 14, 3

DOE O 471.2a, *Information Security*, 11

DOE O 5610.2, *Control of Weapon Data*, 14, 1

Federal Information Processing Standard 199, *Security Categorization of Federal Information and Information Systems*, 14

Federal Information Security Management Act of 2002, 1

National Industrial Security Program Operating Manual, 1

NIST 800-53 Rev. 1, *Recommended Security Controls for Federal Information Systems*, 19

SC Program Cyber Security Plan, 1

TMR 5, *Interconnected Systems Management*, 10

APPENDIX II: GLOSSARY

Assurance Controls. Controls implemented through actions taken by system owners (developers and implementers) of security controls to use state-of-the-practice design, development, and implementation techniques and methods; and actions taken by security control certifiers during the C&A process to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Authenticated User. A user that has been properly identified and authenticated. These are considered legitimate users of the information system.

Common Security Controls. Controls for classified information systems that are applicable to all systems accredited under a Master Security Plan.

Confidential Restricted Data, Sigmas 1 through 13 (CRD1-13). Information that is classified as Confidential and identified as Restricted Data, Formerly Restricted Data, or is related to nuclear weapons contains information that falls in at least one of the sigma categories 1 through 13 as described in DOE O 5610.2, *Control of Weapon Data*, and successors.

Confidential/Secret (C/S) Information. Information that is classified as Confidential National Security Information, Confidential Formerly Restricted Data, Confidential Restricted Data, Secret National Security Information, or Secret Formerly Restricted Data and does not contain any nuclear weapons data.

Configuration (Security-Relevant). The way in which a computer system is set up to meet all security requirements for that system.

Developer. The System Owner responsible for the procurement, development, integration, modification, or operation and maintenance of the information system.

Evaluator. The Certification Agent and/ or the Designated Approving Authority responsible for conducting a comprehensive assessment of the technical, operational, and assurance controls in the information system.

Formerly Restricted Data (FRD). Classified information jointly determined by the DOE or its predecessor agencies and the Department of Defense to be (1) related primarily to the military utilization of atomic weapons and (2) protected as National Security Information. It is subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.

APPENDIX II: GLOSSARY

Information Type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Isolated Network. A group of interconnected systems that are not interconnected with any outside system or across a certification boundary.

National Security Information (NSI). Any information that has been determined, pursuant to Executive Order 12958, *Classified National Security Information,* as amended, or any predecessor order, to require protection against unauthorized disclosure and that is so designated.

National Security System. Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency —

1. the function, operation, or use of which—
    a. involves intelligence activities;
    b. involves cryptographic activities related to national security;
    c. involves command and control of military forces;
    d. involves equipment that is an integral part of a weapon or weapons system; or
    e. is critical to the direct fulfillment of military or intelligence missions; or
2. is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Operational Controls. Controls implemented within the environment in which the information system resides through processes and procedures.

Periods Processing. A system that operates as a standalone system that contains information at varying Protection Levels or need-to-know for the users.

APPENDIX II: GLOSSARY

Protection Level. Contains all information types that require similar protection or are similar in content or use.

Restricted Data (RD). All data concerning design, manufacture, or utilization of atomic weapons; production of special nuclear material; or use of special nuclear material in the production of energy, but excluding data declassified or removed from the Restricted Data category pursuant to 42 U.S.C. 2162 [Section 142, as amended, of the Atomic Energy Act of 1954].

Secret Restricted Data (SRD). Information that is classified Secret Restricted Data and does not contain any nuclear weapons data.

Secret Restricted Data, Sigmas 1 through 13, 15 and 20 (SRD1-13, 15, 20). Information that is classified as Secret and identified as Restricted Data and is related to nuclear weapons and contains information that falls within at least one of the sigma categories 1 through 13, 15 and 20 as described in DOE O 5610.2, *Control of Weapon Data*, and successors.

Secret Restricted Data, Sigmas 1 through 13, 15 and 20 (SRD1-13, 15, 20). Information that is classified as Secret and identified as Restricted Data and is related to nuclear weapons and contains information that falls within at least one of the sigma categories 1 through 13, 15 and 20 as described in DOE O 5610.2, *Control of Weapon Data*, and successors.

Secret Restricted Data, Sigma 14 (SRD14). Information that is classified as Secret and identified as Restricted Data or is related to nuclear weapons and contains information that falls within the Sigma 14 category, as described in DOE O 5610.2, *Control of Weapon Data*, DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Design*, and DOE O 457.1, *Nuclear Counterterrorism*, respectively and their successors.

Security-significant Change. A change to a system's configuration that impacts the security posture of the system. Defined at the site level and approved by the DAA.

Standalone System. A system that does not interconnect with any other system. All processing on the systems is at the same Protection Level and need-to-know for all users.

System Administrator. An authenticated user who has been granted the authority to manage the information system. These users are expected to use this authority only in the manner prescribed by the guidance given them.

APPENDIX II: GLOSSARY

System Owner. The primary contact (Program/Project Manager, primary system user, or data custodian) for an NSS system or network.

Technical Controls. Controls implemented within the information system through means employing software, hardware, or firmware.

Top Secret (TS) Data. Information that is classified as Top Secret National Security Information or Top Secret Formerly Restricted Data and does not contain any nuclear weapons data.

Top Secret Restricted Data (TSRD). Nuclear Weapons information that is classified Top Secret.

APPENDIX III: ACRONYMS

ACREM – Accountable Classified Removable Electronic Media
C&A – Certification and Accreditation
CIRT – Cyber Incident Response Team
CoL – Consequence of Loss
COTS – Commercial Off-the-Shelf
CRD – Confidential Restricted Data
CREM – Classified Removable Electronic Media
C/S – Confidential/Secret
DAA – Designated Approving Authority
DAC – Discretionary Access Controls
DOE – Department of Energy
FIPS – Federal Information Processing Standard
FISMA – Federal Information Security Act of 2002
HLD – High-level Description
ISSM – Information System Security Manager
ISSO – Information System Security Officer
MAC – Mandatory Access Controls
MOU/MOA – Memorandum of Understanding/Memorandum of Agreement
NISPOM – National Industrial Security Program Operating Manual
NIST – National Institute of Standards and Technology
NSS – National Security System
NTC – National Training Center
PCSP – Program Cyber Security Plan
PL – Protection Level
POA&M – Plan of Action and Milestones
Master Plan – Site Cyber Security Program Plan
SIO – Science Information Officer
SP – Security Plan
SO – System Owner
SRD – Secret Restricted Data
TS – Top Secret

APPENDIX III: ACRONYMS

TSRD – Top Secret Restricted Data

APPENDIX IV: COMMON SECURITY CONTROLS

AU-2 Auditable Events

The information system shall provide the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail. The information system shall provide the capability to manage the selection of events to be audited by individual components of the system.

The information system security controls shall generate an audit record of the following events:

- Start-up and shutdown of the audit function
- Successful use of the user security attribute administration functions
- All attempted uses of the user security attribute administration functions
- Identification of which user security attributes have been modified
- Successful and unsuccessful logons and logoffs
- Unsuccessful access to security relevant files including creating, opening, closing, modifying, and deleting those files
- Changes in user authenticators
- Blocking or blacklisting user Ids, terminals, or access ports
- Denial of access for excessive logon attempts
- System accesses by privileged users
- Privileged activities at the system console (either physical or logical consoles) and other system- level accesses by privileged users
- Starting and ending times for each access to the system

AU-3 Audit Record Contents

The audit record for each event shall contain at least the date and time of the event, type of event, user/role, object acted upon, and the outcome (success or failure) of the event

AU-4 Profile Based Anomaly Detection

The audit log provides the capability to determine the historical usage of system resources by individual.

APPENDIX IV: COMMON SECURITY CONTROLS

AU-5 Complex Attack Heuristics

Anti virus software is installed and operational on standalone systems and Intrusion Detection Software (IDS) is installed and operational for networked systems. The system will alert security personnel (e.g., system owner, ISSO, network administrator) of a potential imminent violation of information system security when system activity is found to match a signature event or event sequence that indicates a potential violation of information system security.

AU-6 Audit Review

The system has a mechanism to extract relevant information based on user identification. Network systems checked weekly; standalone systems as part of a forensics investigation. Read access to the audit records shall be prohibited to all users except the ISSO and authorized system administrators. The information system security controls shall provide the ability to perform searches, sorting, and ordering of audit data based on user identity. Audit records shall be reviewed at least weekly and retained for at least one year.

AU-7 Audit Data Availability

The stored audit records shall be protected from unauthorized deletion, prevent modification, and ensure that records already written (i.e. to media) will be maintained when the audit storage is exhausted, the system fails, or an attack occurs. An alarm (e.g. any clear indication that the pre-defined limit has been exceeded) shall be generated and provided to the ISSO and the authorized system administrator if the audit trail storage exceeds 80% of capacity on networked systems. For standalone systems the user will not be able to process work. The information system shall prevent auditable events from being lost (e.g., deleted, overwritten, not recorded), except those taken by the ISSO or authorized system administrator if the audit trail has reached storage capacity.

AU-7(1) Audit Data Availability

The information system shall cease operations if the audit trail has reached storage capacity. The ISSO is the only person authorized to restart operations once sufficient audit capacity is available.

CM-1 Configuration Management System

The system owner shall provide a reference identifier for the information system, use a Configuration Management (CM) system, and provide CM documentation. The reference identifier for the information system shall be unique to each system, and the

information system shall be labeled with its reference. The CM system shall uniquely identify all configuration items. The CM documentation shall include a configuration list that describes the configuration items that comprise the information system and the method used to uniquely identify the configuration items.

The certifier, during the C&A process, shall confirm that the documentation provided meets all the requirements for content. The CM documentation shall include a CM plan that describes how the CM system is used. The CM system shall provide measures such that only authorized changes are made to configuration items. The C&A process shall demonstrate that the CM system is operating in accordance with the plan and documentation shows that all configuration items have been and are being effectively maintained under the CM system.

CM-2 Configuration Management Documentation

The organization authorizes, documents, and controls changes to the information system. The organization:

- Documents proposed changes to the information system;
- Notifies appropriate approval authorities;
- Highlights approvals that have not been received in a timely manner;
- Inhibits change until necessary approvals are received; and
- Documents completed changes to the information system

The certifier, during the C&A process, shall confirm that the documentation provided meets all the requirements for the content.

***CM-5(1) Access Restrictions for Change**

The organization:

- Approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and
- Generates, retains, and reviews records reflecting all such changes. The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

***CM-8(2) Information System Component Inventory**

APPENDIX IV: COMMON SECURITY CONTROLS

The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information. The organization employs mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

DO-1 Delivery Procedures

The ISSO shall document procedures for delivery of the information system or parts of it to the user and shall use the delivery procedures. The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the information system or updates to the user's site.

The certifier, during the C&A process, shall confirm that the documentation provided meets all the requirements for the content.

DP-1 Complete Access Control

The information system implements the access controls correctly for all users (subjects) of the system, including read, write, create, update, and delete for the databases/files (objects) within the system. The DAC security policy shall apply to all operations between any object and subject within the information system. Any named object that is not controlled by the DAC security policy must be justified in the SSP.

DP-2 Security Attribute Based Access Control

The information system security controls shall enforce the DAC security policy to objects based on the user identity and group memberships associated with a subject; and the following access control attributes associated with an object (e.g., identity of users, subjects, or objects; time restrictions; group membership). The DAC defines "subject" as users or user groups, and "objects" as file servers, database, print servers, etc, and shall enforce the security policy based on group membership associated with a subject. The access control attributes must provide the ability to associate allowed or denied operations with one or more user identities; the ability to associate allowed or denied operations with one or more group identities; and defaults for allowed or denied operations.

In addition to the rules specified in DP-1, the information system security controls shall ensure that the DAC policies work as intended, and apply to all subject and objects in the information system. For each operation, there shall be a DAC rule, or rules, that use:

- The permission attributes where the user identity of the subject matches a user identity specified in the access control attributes of the object;

APPENDIX IV: COMMON SECURITY CONTROLS

- The permission attributes where the group membership of the subject matches a group identity specified in the access control attributes of the object; and
- The default permission attributes specified in the access control attributes of the object when neither a user identity nor group identity matches.

The DAC is implemented to assure that everyone (subjects) is not entitled to have all access to all resources (objects). The PCSP or SSP must list the attributes that are used by the DAC policy for access decisions.

DP-6 Subset Information Flow Control

The DAC security policy shall be enforced on subjects (e.g., users, machines, processes), information (e.g., email, files, specified network protocols), and operations that cause controlled information to flow to and from controlled subjects covered by DAC. All subjects and objects are tied either one to one or one to many.

DP-7 Simple Security Attributes

The information system security controls shall enforce the DAC security policy based on the following types of subject and information security attributes: user ID, group ID, file permission bits. The information system security controls shall permit an information flow between a controlled subject and controlled information via a controlled operation if the security attribute-based relationship between the subject and object holds. The information system security controls may explicitly authorize or deny an information flow based on security attribute-based relationship between the subject and the object.

DP-9 Import of User Data without Security Attributes

The Operating System (OS) of the workstation or fileserver will be configured to assure that when importing data from outside the control of the information system via authorized means, such as removable media or document scanner, the information system security controls shall enforce the DAC security policy regardless of the security attributes associated with the data. Devices that do not support this function will be isolated from a network via firewall.

DP-11 Full Residual Information Protection

The information system security controls shall ensure that any previous information content of a resource (e.g. cache, RAM, temp file, cookies, deleted page files) is made unavailable upon the allocation of the resource.

DP-12 Stored Data Integrity Monitoring and Action

APPENDIX IV: COMMON SECURITY CONTROLS

The information system assures that only authorized personnel have access to stored information. The information system security controls shall monitor user data stored within the control of the information system for unauthorized modification and unauthorized deletion on all objects. When storing data to persistent storage, the information system shall make use of the underlying error detection/correction mechanisms of the media, and will detect and report failures on re-read. Where a particular persistent storage device does not provide an effective correction facility, the information system shall store data in such a way as to independently compute and validate an appropriate error detection check. Upon detection of a data integrity error, the information system security control shall enter a description of the error in the audit log and issue an alarm.

DV-1 Correspond. Demonstration

The system developer shall provide the ISSO a functional specification for systems other than Commercial Off-the-Shelf (COTS) software. The functional specification shall provide the high-level design. The system owner shall provide the high-level design (HLD) of the information system security controls. The HLD shall be internally consistent; shall describe the structure of the information system security controls in terms of subsystems; shall describe the security functionality provided by each subsystem of the information system security controls; shall identify any underlying hardware, firmware, and / or software required by the information system security controls with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software; shall identify all interfaces to the subsystems of the information system security controls; and shall identify which of the interfaces to the subsystems of the information system security controls are externally visible.

The certifier, during the C&A process, shall confirm that the documentation provided meets all the requirements for content, shall determine that the functional specification is an accurate and complete representation of the information system security functional requirements, and determine that the high-level design is an accurate and complete description of the information system security functional requirements.

***SA-5(1) Information System Documentation**

The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls

employed within the information system with sufficient detail to permit analysis and testing of the controls.

***SA-10 Developer Configuration Management**

The organization requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

EN-1 Malicious Access

Information system security controls shall be implemented to detect, deter, and respond to malicious actions by authenticated users. Malicious actions include installing or use of unauthorized software, attempting to access network resources, change security configurations, etc. as defined in the Code of Conduct.

EN-2 Management of User Identifiers and Authenticators

Authentication credentials shall be protected from unauthorized access during creation, use, and handling. Authenticated user information system access shall be disabled when the user leaves the sponsoring organization, Access Authorization is terminated, loses authorized access (for cause, changes in organization, etc), or upon information system detection of attempts to bypass security. Prior to reuse of an authenticated user identifier, all previous access rights and privileges (including file accesses for that user identifier) shall be removed from the information system. Authenticated user access, contact information, rights, and privileges, to include sponsor, Access Authorization, need-to-know, means for off line contact, mailing address, shall be validated annually.

EN-3 Information Availability

Capabilities and resources shall be provided to allow the information system user to perform data backup at the user's discretion. User and information system data shall be available, or restorable, to meet mission availability requirements. Periodic checking of backup inventory and testing of the ability to restore information shall be accomplished to validate mission availability requirements are met. The organization shall conduct backups of user-level and system-level information (including system state information) contained in the information system. Backups shall be done at least monthly if the information system is used daily.

EN-4 Purging

APPENDIX IV: COMMON SECURITY CONTROLS

The information system components and removable media shall be purged before the items can be reused in another system environment with the same or different accreditation level as the original system components or removable media. All information system components and removable media shall be purged, using Senior DOE Management approved procedures, prior to release for use at a lower classification level, at a lower level of consequence, or outside the information system boundary.

EN-6 Hardware and Software Examination

Information system hardware and software components shall be examined for security impacts to the information system upon installation.

EN-7 Forensics

Procedures shall be established and documented to ensure the identification, collection, and preservation of data (at the system and network level) needed to analyze and reconstruct events resulting from penetration attempts, penetrations, and on-going cyber attacks and/or failures.

EN-10 Marking

Each information system, visual display, and output device shall be marked in accordance with DOE Manual 470.4-4, Section 2.

EN-12 User Notification

This banner or a banner that conveys the same limitations on privacy shall be presented to the user prior to granting access to system resources. All users shall be notified that they are subject to being monitored, recorded, and audited through the use of the following approved warning text:

WARNINGWARNING**WARNING**WARNING**

THIS IS A DEPARTMENT OF ENERGY (DOE) COMPUTER SYSTEM. DOE COMPUTER SYSTEMS ARE PROVIDED FOR THE PROCESSING OF OFFICIAL U.S. GOVERNMENT INFORMATION ONLY. ALL DATA CONTAINED WITHIN DOE COMPUTER SYSTEMS IS OWNED BY THE DOE, AND MAY BE AUDITED, INTERCEPTED, RECORDED, READ, COPIED, OR CAPTURED IN ANY MANNER AND DISCLOSED IN ANY MANNER, BY AUTHORIZED

APPENDIX IV: COMMON SECURITY CONTROLS

PERSONNEL. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. SYSTEM PERSONNEL MAY DISCLOSE ANY POTENTIAL EVIDENCE OF CRIME FOUND ON DOE COMPUTER SYSTEMS TO APPROPRIATE AUTHORITIES. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS AUDITING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, AND DISCLOSURE OF COMPUTER ACTIVITY.

WARNINGWARNING**WARNING**WARNING**

Explicit acknowledgement of the warning by the user is required before granting the user access to system resources.

EN-13 Need-to-Know

Prior to their first access to information, each user's need-to-know shall be formally authorized by management, the data owner, or the data-steward.

EN-14 Physical Security

Access controls shall ensure that personnel granted unescorted physical access to the information, the information system, or human readable media have the appropriate access authorization, formal access approval, and need-to-know. Physical attack, which might compromise security, on those parts of the information system critical to security shall be deterred and detected.

EN-15 Physical Access Protection

The information system shall be protected by being constantly attended and under the control of a person that possesses proper access authorization, formal access approval, and need-to-know, or by physical protection, as prescribed for the classification level and category of the information, to restrict access to those with appropriate clearance, formal access approvals, and need-to-know. The information system shall be protected by default setting of disabled/closed, with all ports and/or devices capable of writing to removable or external media being protected from unauthorized modification or use by [describe software and/or hardware means used to prevent unauthorized use or modification of all ports and/or devices capable of writing to removable or external media. When this protection is implemented by software, the named object must be listed in DP-1 and access control rules described in DP-2.

APPENDIX IV: COMMON SECURITY CONTROLS

EN-19 Media and Component Review

The organization:

- Affixes external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and
- Exempts from labeling all media so long as they remain within protected environment.

All media (paper, disks, zip drives, removable disk drives, etc.) shall be reviewed by an authorized derivative classifier for sensitivity and properly marked before release outside the system boundary.

EN-20 User Access Right and Privileges

User must log on with the least privileges to do the job. The data owner defines the need to know and operational requirements for the users. ISSO determines the privileges needed to accomplish the task.

EN-21 Security Roles

The same person must not perform the functions of implementing security changes and security approval of said changes. Other roles involved with security administration, such as DBMS administration, must not performed by the same person performing the change and the approval. All system administrators must sign and adhere to a Code of Conduct agreement which outlines their responsibilities with regard to being granted privileged access to NSS.

EN-22 Two-Person Rule

Two security-trained and technically knowledgeable people approved by the ISSM or DAA (e.g. ISSO and system administrator) shall be present when audit parameters or audit file contents are modified.

EN-23 User Training

All authenticated users shall be trained to understand applicable information system use policies, the approved use of the information system, the vulnerabilities inherent in the operation of the information system, and their cyber security responsibilities.

EN-24 User Clearance

APPENDIX IV: COMMON SECURITY CONTROLS

All users (including privileged users) shall possess a current Access Authorization prior to their first access to the information system.

EN-24(1) User Clearance

For PI-1 and PI-3, all users shall, at a minimum, possess a current "L" Access Authorization.

EN-24(2)

User Clearance For PI-2 and PI-4 through PI-7, all users shall, at a minimum, possess a current "Q" level access authorization.

EN-25 National Security Systems Workstations

Workstations shall be prohibited from reading from, or writing to, removable media without appropriate security controls, including system-level intervention to permit unique read/write events. The security controls and unique read/write events shall be documented in the security plan. Diskless workstations located within an open area shall not retain any data remnants upon power off (other than simple BIOS).

GD-1 Administrator Guidance

The system owner shall provide the system administrator a system security document that outlines the functional requirements and protections required for the system.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

GD-2 User Guidance

The system owner shall provide user guidance. The user guidance shall describe the functions and interfaces available to the non-administrative users of the information system; shall describe the use of user-accessible security functions provided by the information system; shall contain warnings about user accessible functions and privileges that should be controlled in a secure processing environment; shall clearly present all user responsibilities necessary for the secure operation of the information system, including those related to assumptions regarding user behavior found in the statement of the information system security environment; shall be consistent with all other documentation supplied for evaluation; and shall describe all security requirements for the IT environment that are relevant to the user.

APPENDIX IV: COMMON SECURITY CONTROLS

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

IA-1 Authentication Failure Handling

The information system security controls shall detect when no more than three (3) consecutive unsuccessful authentication attempts occur related to the last successful session authentication for the indicated user. When the defined number of unsuccessful authentication attempts has been met or surpassed, the information system security controls shall inform the system administrator and disable the user account until it is unlocked by the administrator. Standalone systems that do not have notification systems should be set to lock user and note in audit log.

IA-10 User-Subject DAC Binding

The DAC shall establish a set of rules between the users (subjects) and the system resources (objects) with respect to what the uses can do with those objects. (e.g. read, write, create, delete, edit). The information system shall record user activities in the event logs.

IA-2 User Attribute Definition

The information system security controls shall maintain the security attributes of user identifier, group memberships, authentication data, and security-relevant role for individual users.

IA-4 Timing of Authentication

The information system security controls shall allow no actions on behalf of the user to be performed before the user is authenticated. However, each user shall be successfully authenticated before allowing any other information system security controls mediated actions.

IA-6 Re-authentication

The information system security controls shall require re-authentication of the user under the conditions of unlocking as a result of locking.

IA-7 Protected Authentication Feedback

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

APPENDIX IV: COMMON SECURITY CONTROLS

IA-8 Timing of Identification

The information system security controls shall allow , no actions on behalf of the user to be performed before the user is identified.

IA-9 User Identification Before Any Action

The information system security controls do not allow guest or anonymous users to have access to system resources.

LC-1 Identification of Security Measures

The ISSO/ISSM shall produce the program and system security plans. The system security plan shall describe all physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the information system design and implementation in its development environment and shall provide evidence that these security measures are followed during the development and maintenance of the information system.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content and shall confirm that the security measures are being applied.

LC-2 Flaw Remediation

Flaws in COTS hardware or software may adversely affect the confidentiality, availability, or integrity of national security information. Flaws may be identified through a variety of means, such as vendor notifications, vulnerability analysis, or certification testing. The system owner shall document the flaw remediation procedures. The flaw remediation procedures documentation shall describe the procedures used to patch operating system and application software vulnerabilities, update virus signature files, or modify the configuration settings of the targeted device. The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided as well as the status of finding a correction to the flaw and shall require that corrective actions be identified for each of the security flaws.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

LC-2(1) Flaw Remediation

The system owner shall designate one or more specific points of contact for user reports and inquiries about security issues involving the information system. The flaw

remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw. The flaw remediation guidance shall describe a means by which information system users may register with the system owner, to be eligible to receive security flaw reports and corrections. The flaw remediation guidance shall identify the specific points of contact for all reports and inquiries about security issues involving the information system.

LC-2a Flaw Remediation

The system owner shall establish a procedure for accepting and acting upon vendor reports of security flaws and shall provide flaw remediation guidance addressed to information system users. The flaw remediation procedures documentation shall describe a means by which the system owner receives vendor reports of suspected security flaws in the information system. The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to information system users and shall provide safeguards that any corrections to these security flaws do not introduce any new flaws. The flaw remediation guidance shall describe a means by which information system users report to the system owner any suspected COTS security flaws in the information system and a means for verification that suspected security flaws are addressed.

LC-3 Defined Life Cycle Model

The system owner shall establish a life-cycle model to be used in the development and maintenance of the information system and shall provide life-cycle definition documentation. The life-cycle definition documentation shall describe the model used to develop and maintain the information system and the life-cycle model shall provide for the necessary control over the development and maintenance and decommission of the information system.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

MT-1 Management of Security Functions Behavior

The information system security controls limit access and changes to the security functions (configuration setting, audit logs, etc) to ISSOs and authorized systems administrators.

MT-2 Management of Security Attributes

APPENDIX IV: COMMON SECURITY CONTROLS

The information system security controls limit access and changes to the Access Control List (ACL) to ISSOs and authorized systems administrators.

MT-3 Static Attribute Initialization

The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: peer to peer, anonymous FTP. The organization reviews the information system (if standalone -once every six months), to identify and eliminate unnecessary functions, ports, protocols, and/or services.

MT-4 Management of Security Data

The information system security controls shall permit only authorized SA and ISSOs to modify (delete/clear) the audit logs, or change other authentication data (e.g. passwords).

MT-4(1) Management of Security Data

The information system security controls shall permit only authorized SA and ISSOs to change the system time.

MT-5 Revocation

The information system security controls shall assure only the ISSO and authorized system administrators that can revoke security attributes associated with the users within the information system. The information system security controls shall enforce the revocation of the attributes in real time (if a standalone system - upon system reboot). Upon revocation of security-relevant authorizations (e.g., disable subject) the system must reassign ownership of objects, to approved subjects within the information system. The information system security controls shall enforce the access rights associated with an object when an access check is made.

MT-6 Restriction on Security Roles

The information system security controls shall be able to associate users with roles and shall maintain the roles of ISSO, authorized system administrator, and users explicitly authorized by the DAC security policy to modify object security attributes and their own authentication data (e.g., passwords). The information system security controls shall ensure that the conditions of least privilege are satisfied. If a user has been granted system administrator privileges, then the user will use this role only to perform system administrator functions.

APPENDIX IV: COMMON SECURITY CONTROLS

PT-1 Information System Security Control Testing

The information system controls shall run a suite of self-tests (e.g., Power-On Self Test) during initial start-up, periodically during normal operation, or at the request of the authorized user (e.g., recovery from failed condition/event) to demonstrate the correct operation of the information system security controls.

PT-3 Information System Recovery

The organization employs manual or automated mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

PT-5 Non-bypassability of the Security Policy

The information system security controls shall ensure that the information system security policy enforcement functions (e.g. role based access controls) are invoked and succeed before each function within the information system's control is allowed to proceed.

PT-6 Domain Separation

The un-isolated portion of the information system security controls shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects and shall enforce separation between the security domains of subjects under the control of the information system. The information system security controls shall maintain the part of the information system security controls related to the DAC security policy in a security domain for their own execution that protects them from interference and tampering by the remainder of the information system's controls and by subjects untrusted with respect to those DAC security policy. If third party software is applied as a security control it is set so that only the administrator may change the software setting.

PT-7 Reliable Time Stamps

The information system security controls shall be able to provide reliable time stamps for its own use.

PT-8 Fail Secure

The information system shall fail to a "secure" state, defined in the SSP, in which the security functions of the data are consistent and the security functions continue correct enforcement of the security policy. The SSP shall also specify those situations in which

audit is desired and feasible from the "secure" state. Failures in the security function may include "hard" failures, which indicate an equipment malfunction and may require maintenance, service or repair of the security function. Failures in the security function may also include recoverable "soft" failures (e.g., failure of the integrity of information system security control data, initialization or resetting of the security function, etc.).

SA-2 Session Locking and Termination

The information system security controls prevents further access to the system by initiating a session lock after maximum of 15 minutes) of inactivity and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. The information system automatically terminates a remote session after 15 minutes after session lock period initiates of inactivity.

SA-3 Default Access Banners

The information system displays an approved, system use notification message before granting system access informing potential users:

- That the user is accessing a Department of Energy (DOE) computer system. DOE computer systems are provided for the processing of official U.S. Government information only. All data contained within DOE computer systems is owned by the DOE, and
- That system usage may be audited, intercepted, monitored, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. (See EN-12 for the sample warning text.)

The notification message and remains on the screen until the user takes explicit actions to log on to the information system.

SA-4 Information System Access History

The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

TE-1 Test Coverage

The system owner shall provide evidence of the test coverage. The evidence of test coverage shall show the correspondence between the test identified in the test documentation and the information system security controls as described in the functional specification.

APPENDIX IV: COMMON SECURITY CONTROLS

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

TE-1(1)Test Coverage

The ISSO shall provide an analysis of test coverage. The analysis of test coverage shall demonstrate the correspondence between the test identified in the test documentation and the information system security controls as described in the functional specification and between the information system security controls as described in the functional specification and the tests identified in the test documentation is complete. A gap report and POA&M list will be prepared as evidence of this control, if required.

TE-2 Testing

The ISSO shall test the information system security controls and document the results. The system owner shall provide test documentation that consists of test plans, test procedure descriptions, expected test results, and the actual test results. The test plans shall identify the security controls to be tested and describe the goal of the tests to be performed. The test procedures shall identify the test to be performed and describe the scenarios for testing each security function. The scenarios shall include any ordering dependencies on the results of other tests. The expected test results shall show the anticipated outputs from a successful execution of the tests. The test results from the system owner execution of the tests shall demonstrate that each tested security control behaved as specified. The system owner shall provide a suitable information system for testing and shall provide an equivalent set of resources to those that were used in the system owner's functional testing of the information system security controls.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content, shall select and test a subset of the information system security controls as appropriate to confirm that the information system operates as specified, and shall execute a sample of tests in the test documentation to verify the system owner test results.

TE-2(1)Testing

The system owner shall provide the analysis of the depth of testing. The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the information system security controls operates in accordance with its high-level design (e.g. which controls were tested via interview, observation or functional test).

VA-1 Vulnerability Analysis

APPENDIX IV: COMMON SECURITY CONTROLS

The system administrator or ISSO shall perform and document an analysis of the information system deliverables searching for obvious ways in which a user can violate the information system security policy. The system owner shall document the disposition of the obvious vulnerabilities and the documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the information system.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content and shall conduct penetration testing, building on the system owner vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

VA-1(1) Vulnerability Analysis

The system administrator or ISSO shall document the disposition of identified vulnerabilities (e.g. when the system was last updated for virus signatures or patched). The organization updates the list of information system vulnerabilities scanned when significant new vulnerabilities are identified and reported. The documentation shall justify that the information system, with the identified vulnerabilities, is resistant to obvious penetration attacks.

The certifier, during the C&A process, shall perform an independent vulnerabilities analysis; shall perform independent penetration testing based on the independent vulnerability analysis to determine the exploitability of additional identified vulnerabilities in the intended environment; and shall determine that the information system is resistant to penetration attacks performed by an attacker possessing a low attack potential.

VA-2 Examination of Guidance

The ISSO shall provide the ISSM with the complete Certification and Accreditation documentation suite. The documentation shall identify all possible modes of operation of the information system (including operation following failure or operational error), their consequences and implications for maintaining secure operations. The documentation shall be complete, clear, consistent, and reasonable; shall list all assumptions about the intended environment; and list all requirements for external security measures (including external procedural, physical and personnel controls).

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for content, shall repeat all configuration and installation procedures to confirm that the information system can be configured and used securely

using only the supplied guidance documentation, and shall determine that the use of the guidance documentation allows all insecure states to be detected.

VA-2(1) Examination of Guidance

The ISSO shall provide the ISSM with a gap analysis and POA&M list (if required) that demonstrates the C&A documentation is complete and ready for the DAA to review.

The certifier, during the C&A process, shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the information system.

***MA-3(1) Maintenance Tools**

The organization must define a process to approve, control, and monitor the use of information system maintenance tools and maintains the tools on an ongoing basis within the controlled area. The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.

***MA-4(3) Remote Maintenance**

The organization must define a process to authorize, monitor, and control any remotely executed maintenance and diagnostic activities, if employed. The organization does not allow remote maintenance or diagnostic services to be performed by a provider that does not implement for its own information system, a level of security at least as high as that implemented on the system being serviced, unless the component being serviced is removed from the information system and sanitized (with regard to organizational information) before the service begins and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system.

***MP-6(1) Media Sanitization and Disposal**

The organization must define a process to purge information system media, both digital and non-digital, prior to disposal or release for reuse. The organization tracks, documents, and verifies media sanitization and disposal actions. Tracking is for Accountable media. See DOE 470.4-4 chapter II.4.

***PE-18(1) Location of Information System Components**

The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. The organization plans the location or site of

the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

***PE-4 Access Control for Transmission Medium**

The organization controls physical access to information system distribution and transmission lines within organizational facilities in accordance with 205.1-3.

APPENDIX V: STANDALONE PERIODS PROCESSING SECURITY CONTROLS

IA-3 Verification of Secrets

The information system security controls shall provide a mechanism to verify that secrets meet at least two-factor strong authentication mechanisms prior to granting access to systems and the information and resources managed by that system. Two-factor authentication must consist of (2 of 3) something you know, something you have or something you are. For stand-alone systems "something you have" is the drive itself.

IA-5 Multiple Authentication Mechanisms

The information system security controls may provide passwords; fingerprints; smart cards or other nationally recognized approved mechanism to support user authentication. For systems not connected to a network, the information system security controls for two factor authentication will include physical access control to the safe which contains the disk of classified information. Multi factor authentication will consist of “access to the limited area", knowledge of the safe combination, and logon ID/password to the system. For networked systems, two-factor shall include something you have (e.g., a token or fingerprint) combined with something you know (e.g., password).

APPENDIX VI: ISOLATED NETWORK SECURITY CONTROLS

AU-1 Security Alarms

The information system security controls shall include or exclude auditable events from the set of audited events based on the user identity and role and shall automatically alert the Information System Security Officer (ISSO) and/or the System Administration and take automatically lock out the system/user, or isolate the system/user upon detection of a potential security violation. Notification is through lockout and audit log entry for systems not connected to a network with alerting capability.

AU-3(2) Audit Record Contents

The information system shall synchronize internal information system clocks at least daily.

AU-4(1) Profile Based Anomaly Detection

The information system shall have the ability to centralize the analysis of the logs and employ software filters to do the first level sorts/analysis. The information system shall employ automated mechanisms (e.g. writing to audit log file, issuing alarms to a network console) to alert security personnel of excessive login attempts across network; access to privilege system files, exceeding data quotas/transfers, creation of account; privileged account logged into multiple servers/ devices/applications; attempts to access unauthorized sites/computers/devices/objects; unauthorized shutdown/restart of system/device/application; permission change for user/file/application; use of privileged commands; and unauthorized export from system to media).

CS-1 Crypto Key Establishment and Management

When cryptography is required and used within the information system for other than telecommunications, the information system security controls shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures. The requirements in DOE Manual 205.1-3, Telecommunications Security Manual, must be implemented for telecommunications systems. If cryptographic keys are not used, this should be stated in the SSP.

CS-2 Crypto Operation

When cryptography is required and used within the information system for other than telecommunications ,the information system security controls shall perform cryptographic operations (e.g., password encryption, e-mail encryption, etc.) that meet FIPS 140-2. The requirements in DOE M 205.1-3, Telecommunications Security Manual,

APPENDIX VI: ISOLATED NETWORK SECURITY CONTROLS

must be implemented for telecommunications systems. If cryptographic keys are not used this should be stated in the SSP.

DP-3 Basic Data Authentication

The information system security controls shall provide a capability to generate evidence (cryptographic checksum, message digest) that can be used as a guarantee of the validity of files, e-mail messages, software load, etc and shall provide user or processes acting on behalf of users with the ability to verify evidence of the validity of the indicated information.

EN-8 Intrusion Detection

The site and network (when applicable) environment shall provide the ability to detect (i.e., using methods readily available on the Internet to attack known vulnerabilities) and sophisticated attacks on the network, network components, and hosts from inside or outside the site, including measures to detect and respond to unauthorized attempts to penetrate or deny use. For systems that are not networked, audit logs and physical access records may be acceptable compensatory controls.

EN-11 Interconnected Environment

The information system must provide the ability to specify and manage user access rights to the information system and data resources (i.e. access authorization through the network), supporting the organization's security policy for access control.

EN-16 Environmental Protection

The information system environment shall be capable of physically protecting the information system and components stored in a remote location by signaling the occurrence of fire, flood, power loss, and environmental control failures that might adversely affect information system operations.

EN-17 Information Protection

Information protection shall be required whenever national security information is to be transmitted through components or areas where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media. One or more of the following methods approved through the Senior DOE Management PCSP for the level and category of information must be used to protect the information in transit [i.e., information

APPENDIX VI: ISOLATED NETWORK SECURITY CONTROLS

distributed only within an area approved for open storage of the information; National Security Agency (NSA) approved Type I encryption mechanisms; DOE approved encryption mechanisms; or DOE approved Protected Transmission Systems].

EN-18 System Recovery

All remote terminal access must be monitored and controlled when used for system recovery operations.

PT-4 Replay Detection

The information system security controls shall detect replay for [list of identified entities (e.g., messages, service requests, service responses, and user sessions)] and shall perform [list of specific actions (e.g., ignoring the replayed entity, requesting confirmation of the entity from the identified source, and terminating the subject from which the re-played entity originated)] when replay is detected.

SA-1 Concurrent Session Limitations

The information system security controls the number of concurrent sessions for any user to [site-defined number of sessions].

APPENDIX VII: NETWORKED SYSTEM SECURITY CONTROLS

EN-9 Information System Interface

The information system must have perimeter protection that implements a managed interface with any external connection, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted. The information system denies information flow by default and allows information flow by exception (i.e., deny all, permit by exception). The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

PT-2 Information System Security Control Data Transmission

The information system protects the integrity of transmitted information. The organization employs cryptographic mechanisms in accordance with DOE 205.3-1 to recognize changes to information during transmission unless otherwise protected by alternative physical measures. The information system must incorporate an NSA-approved secure tunneling capability between systems to protect information from unauthorized disclosure during transmission.

TP-1 Trusted Path

The information system must incorporate a distinct NSA-approved secure device between communication paths to protect information from unauthorized disclosure during transmission.

APPENDIX VIII: PL 5-7 SECURITY CONTROLS

AU-2(1) Auditable Events

The information system security controls shall generate an audit record of the creation, deletion, or change of a security label. The information system shall be able to include or exclude auditable events from the set of audited events based on the subject sensitivity label; object sensitivity label; and source host identity.

AU-3(1) Audit Record Contents

The information system security controls shall record within each audit record for each audit event the sensitivity labels of subject, object, the information involved (e.g. file or records accessed), and the source host identity (e.g. MAC/IP or computer name of the host system).

AU-6(1) Audit Review

The information system security controls shall provide the ability to perform searches, sorting, and ordering of audit data based on subject sensitivity label, object sensitivity label, and source host identity.

CM-1(1) Configuration Management System

The CM documentation shall include an acceptance plan that describes the procedures used to accept modified or newly created configuration items. The CM system shall support the generation of the information system, provide an automated means by which only authorized changes are made to the information system and CM implementation representation, and describe the automated tools used in the CM system.

CM-2(1) Configuration Management Documentation

The CM documentation shall show that the CM system tracks security flaws.

CO-1 Proof of Origin

The system must be able to support digital signatures. The information system security controls shall be able to generate evidence of origin for transmitted information types (e.g., Confidential/Secret, Secret RD, Confidential RD, Secret RD 1-13, etc).at the request of the originator, recipient, ISSO, or third parties (e.g., system owner, ISSM, project management, etc.) and provide a capability to verify the evidence of origin of information to the originator, recipient, or third parties given the limitations on the evidence of origin (e.g., access authorization, formal access authorization, need-to-know, etc.). The information system security controls shall be able to relate the identity of user,

APPENDIX VIII: PL 5-7 SECURITY CONTROLS

level/category of information and attributes (e.g., user ID, authorized, labels authorized, permission attributes) of the originator of the information and the information fields (e.g., header information, IP addresses, etc.) of the information to which the evidence applies.

CO-2 Proof of Receipt

The system must be able to support third party digital signature exchange. The information system security controls shall be able to generate evidence of receipt for received information types (e.g., Confidential/Secret, Secret RD, Confidential RD, Secret RD 1-13, etc) at the request of the originator, recipient, ISSO, or third parties (e.g., system owner, ISSM, project management, etc.) and provide a capability to verify the evidence of origin of information to the originator, recipient, or third parties (e.g., system owner, project management, etc.) given the limitations on the evidence of origin (e.g., access authorization, formal access authorization, need-to-know, etc.). The information system security controls shall be able to relate the attributes (e.g., user ID, authorized, labels authorized, permission attributes) of the recipient of the information, and the information fields (e.g., header information, IP addresses, etc.) of the information to which the evidence applies.

DO-2 Installation, Generation and Startup Procedures

The system owner (vendor) shall document procedures necessary for the secure installation, generation, and startup of the information system. The documentation shall describe the steps necessary for secure installation, generation, and start-up of the information system. The documentation shall confirm that the information provided meets all requirements for content.

The certifier, during the C&A process, shall determine that the installation, generation and startup procedures result in a secure configuration.

DP-10 Import of User Data with Security Attributes

The information system security controls shall enforce the MAC security policy; wherein sensitivity labels consist of a hierarchical level and set of non-hierarchical categories when importing labeled user data from outside the control of the information system. The information system security controls shall ensure that the protocol used provides for the unambiguous association between security attributes and the labeled user data received and that interpretation of the security attributes of the imported labeled user data is as intended by the source of the user data. The sensitivity labels on information must match on input and output of information. The information system security

controls shall use the security attributes associated with the imported labeled user data and shall enforce the following rules when user data is imported from the control of the information system:

- Devices used to import data with security attributes cannot be used to import data without security attributes unless the change in device state is performed manually and is auditable.
- Devices used to import data with security attributes shall completely and unambiguously associate the security attributes with the corresponding data.

DP-11(1) Full Residual Information Protection

The information systems security controls shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to all subjects.

DP-4 Export of User Data without Security Attributes

The information system security controls shall enforce the Mandatory Access Control (MAC) security policy and that devices used to export data without security attributes cannot be used to export data with security attributes unless the change in device state is performed manually and is auditable when exporting unlabeled user data, controlled under the MAC policy, outside the control of the information system. Single-level Input/ Output devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. When data is exported in human-readable or printable form, the authorized administrator shall be able to specify the printable label that is assigned to the sensitivity label associated with the data; each print job shall be marked in accordance with DOE Classified Matter Protection and Control (CMPC) requirements. When data is exported on removable media, the media must be marked in accordance with DOE CMPC requirements.

DP-5 Export of User Data with Security Attributes

The information system security controls shall enforce the Mandatory Access Control (MAC) security policy when exporting labeled user data, controlled under the MAC security policy when exporting, outside the control of the information system by exporting the user data with the user data's associated security attributes (e.g., the classification of the data must be displayed on the media when printed out). The information system security controls shall ensure that the security attributes, when exported outside the control of the information system, are unambiguously associated

with the exported user data and shall enforce the following rules when user data is exported from the control of the information system:

- When data is exported in a human-readable or printable form the authorized administrator shall be able to specify the printable label that is assigned to the sensitivity label associated with the data; each print job shall be marked in accordance with DOE CMPC requirements.
- When data is exported on removable media, the media must be marked and protected in accordance with DOE CPMC requirements.
- Devices used to export data with security attributes cannot be used to export data without security attributes unless the change in device state is performed manually and is auditable.
- Devices used to export data with security attributes shall completely and unambiguously associate the security attributes with the corresponding data.

DP-6(1) Subset Information Flow Control

The MAC security policy shall be enforced on [list of subjects (e.g., users, machines, processes), information (e.g., email, files, specified network protocols), and operations that cause controlled information to flow to and from controlled subjects covered by the MAC.

DP-8 Hierarchical Security Attributes

The information system security controls shall enforce MAC security policy based on the sensitivity label of the subject and sensitivity label of the object containing the information. The sensitivity label of subjects and objects shall consist of a hierarchical level and a set of non- hierarchical categories. The information system security controls may explicitly authorize or deny an information flow based on [rules, based on security attributes, which explicitly authorize or deny information flows].The information system security controls shall permit an information flow between a controlled subject and controlled information via a controlled operation, based on the ordering relationships between security attributes.

- If the sensitivity label of the subject (e.g., DOE Q clearance with additional Sigma authorizations) is greater than or equal to the sensitivity label of the object, then the flow of information from the object to the subject is permitted (a read operation);

APPENDIX VIII: PL 5-7 SECURITY CONTROLS

- If the sensitivity label of the object is greater than or equal to the sensitivity label of the subject; then the flow of information from the subject to the object is permitted (a write operation); or

- If the sensitivity label of subject A is greater than or equal to the sensitivity label of subject B; then the flow of information from subject B to subject A is permitted. The information system security controls may explicitly authorize or deny an information flow based on [rules, based on security attributes, which explicitly authorize or deny information flows].

The information system security controls may explicitly authorize or deny an information flow based on [rules, based on security attributes, which explicitly authorize or deny information flows].

DP-9(1) Import of User Data without Security Attributes

The information system security controls shall enforce the MAC security policy when importing user data, controlled under the MAC security policy, from outside of the control of the information system. Devices used to import user data, controlled under MAC security policy, without security attributes cannot be used to import data with security attributes unless the change in device state is performed manually and is auditable. Security attributes shall be assigned to data upon import to the information system.

DV-1(1) Correspond. Demonstration

For custom developed (not COTS) software, the HLD shall describe the purpose and method of use of all interfaces to the subsystems of the information system security controls, providing details of effects, exceptions, and error messages, as appropriate and shall describe the separation of the information system into security control-enforcing components and other subsystems.

DV-2 Implementation of the information System Controls

The software developer shall provide the implementation representation for a selected subset of the information system security controls. The implementation representation shall unambiguously define the information system security controls to a level of detail such that the information system security controls can be generated without further design decisions. The implementation representation shall be internally consistent.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content and presentation of evidence and determine that

APPENDIX VIII: PL 5-7 SECURITY CONTROLS

the least abstract information system security controls representation provided is an accurate and complete instantiation of the information system security functional requirements.

DV-3 Information System Security Policy Model

The software developer shall provide an information system security policy model. The software developer shall demonstrate correspondence between the functional specification and the information system security policy model. The information system security policy model shall describe the rules and characteristics of all policies of the information system security policy that can be modeled and include a rationale that demonstrates that it is consistent and complete with respect to all policies of the information system security policy that can be modeled. The demonstration of correspondence between the information system security policy model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the information system security policy model.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

EN-5 Covert Channels

The information system must be reviewed to identify covert channels.

EN-6(1) Hardware and Software Examination

Information system hardware components shall be examined to validate the chip sets and boards are from the manufacturer before use. Information system software components shall be examined and tested to determine if the software conforms to security relevant controls as documented by the system owner and contains no malicious code before use.

EN-6(2) Hardware and Software Examination

Information system hardware components shall be examined by manufacturer diagnostics to confirm the information system chip sets and boards function as expected before use. Information system software components shall be examined and tested to determine if controls can be bypassed before use.

IA-11 User-Subject MAC Binding

APPENDIX VIII: PL 5-7 SECURITY CONTROLS

The information system security controls shall associate the user security attribute of sensitivity label, consisting of a hierarchical level and a set of non-hierarchical categories, used to enforce the MAC security policy which with subjects acting on behalf of that user. The information system security controls shall enforce the following additional rule on the initial association of user security attributes with subjects acting on behalf of that user: the sensitivity label associated with a subject shall be within the clearance range, and the clearance level and formal access approvals of the user.

IA-2(1) User Attribute Definition

The information system security controls shall maintain the security attribute of security clearances and formal access approvals for the individual users.

MT-2(1) Management of Security Attributes

The information system security controls shall enforce the MAC security policy to restrict the ability to modify the security attributes sensitivity label associated with an object to the ISSO and users authorized by the ISSO. The information system must immediately notify the user of each change in the security level or compartment associated with that user during an interactive session.

MT-3(1) Static Attribute Initialization

The information system security controls shall enforce the MAC security policy to provide restrictive default values for security attributes that are used to enforce the MAC security policy. The information system security controls shall allow the ISSO and users authorized by the ISSO to specify alternative initial values to override the default values when an object or information is created.

MT-5(1) Revocation

The rules of the MAC security policy (DP-6) are enforced on all future operations.

MT-6(1) Restriction on Security Roles

The information system security controls shall also maintain the role of users authorized by the MAC security policy to modify object security attributes.

SA-5 Deny Session Establishment

The information system security controls shall be able to deny session establishment based on at a minimum user's identity, clearance level, integrity level, membership in a role.

APPENDIX VIII: PL 5-7 SECURITY CONTROLS

PT-2(1) Information System Security Control Data Transmission

The information system security controls shall protect information system security control data from disclosure when it is transmitted between separate parts (components) of the information system.

PT-6(1) Domain Separation

The information system security controls shall maintain the part of the information system security controls related to the DAC and MAC security policies in a security domain for their own execution that protects them from interference and tampering by the remainder of the information system security controls and by subjects untrusted with respect to those DAC or MAC security policies.

RU-1 Quotas

The information system security controls shall enforce maximum quotas of [list of controlled resources (e.g., file servers, disk drives, print spoolers, etc.)] that an individual user, defined group of users, subjects can use simultaneously and/or over a specified period of time.

RU-1(1) Quotas

The information system security controls shall enforce minimum quotas of [list of controlled resources (e.g., file servers, disk drives, print spoolers, etc.) that an individual user, defined group of users, or subjects can use simultaneously and/or over a specified period of time.

***PE-6(2) Monitoring Physical Access**

The organization monitors physical access to the information system to detect and respond to physical security incidents. The organization employs automated mechanisms (cameras, access controlled doors) to recognize potential intrusions and initiate appropriate response actions

***PE-8(2) Access Records**

The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes:

- Name and organization of the person visiting;
- Signature of the visitor;

APPENDIX VIII: PL 5-7 SECURITY CONTROLS

- Form of identification;
- Date of access;
- Time of entry and departure;
- Purpose of visit; and
- Name and organization of person visited.

Designated officials within the organization review the visitor access records [Assignment: organization-defined frequency]. The organization maintains a record of all physical access, both visitor and authorized individuals.

***SA-5(2) Information System Documentation**

The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

APPENDIX IX: SUPPLEMENTAL CONTROLS FOR INTEGRITY AND AVAILABILITY

***CM-6(1) Configuration Settings**

The organization:

- Establishes mandatory configuration settings for information technology products employed within the information system;
- Configures the security settings of information technology products to the most restrictive mode consistent with operational requirements;
- Documents the configuration settings; and
- Enforces the configuration settings in all components of the information system.

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings

***CP-10(1) Information System Recovery and Reconstitution**

The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure. The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.

***CP-2(2) Contingency Plans**

The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel. The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.

***CP-3(1) Contingency Training**

The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training. The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

***CP-4(2) Contingency Plan Testing and Exercises**

APPENDIX IX: SUPPLEMENTAL CONTROLS FOR INTEGRITY AND AVAILABILITY

The organization:

- Tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and
- Reviews the contingency plan test/exercise results and initiates corrective actions.

The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

***CP-7(4) Alternate Processing Site**

The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary processing capabilities are unavailable. The organization fully configures the alternate processing site so that it is ready to be used as the operational site supporting a minimum required operational capability

***CP-8(3) Telecommunications Services**

The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable. The organization obtains alternate telecommunications service providers that are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.

***CP-8(4) Telecommunications Services**

The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable. The organization requires primary and alternate telecommunications service providers to have adequate contingency plans

APPENDIX IX: SUPPLEMENTAL CONTROLS FOR INTEGRITY AND AVAILABILITY

***CP-9(2) Information System Backup**

The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and protects backup information at the storage location. The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.

***CP-9(3) Information System Backup**

The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and protects backup information at the storage location. The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.

***IA-2(2) User Identification and Authentication**

The information system uniquely identifies and authenticates users (or processes acting on behalf of users). The information system employs multifactor authentication for local system access that is NIST Special Publication 800-63 [Selection: organization-defined level 3 or level 4] compliant

***IA-2(3) User Identification and Authentication**

The information system uniquely identifies and authenticates users (or processes acting on behalf of users). The information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 level 4 compliant.

***IR-2(1) Incident Response Training**

The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency, at least annually]. The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

***IR-3(1) Incident Response Testing and Exercises**

The organization tests and/or exercises the incident response capability for the information system [Assignment: organization-defined frequency, at least annually]

using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results. The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.

***IR-5(1) Incident Monitoring**

The organization tracks and documents information system security incidents on an ongoing basis. The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

***MA-2(2) Controlled Maintenance**

The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization employs automated mechanisms to schedule and conduct maintenance as required, and to create up-to date, accurate, complete, and available records of all maintenance actions, both needed and completed

***PE-10(1) Emergency Shutoff**

The organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment. The organization protects the emergency power-off capability from accidental or unauthorized activation

***PE-11(1) Emergency Power**

The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source

***PE-15(1) Water Damage Protection**

The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel. The

organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.

***PE-8(1) Access Records**

The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes:

- Name and organization of the person visiting;
- Signature of the visitor;
- Form of identification;
- Date of access;
- Time of entry and departure;
- Purpose of visit; and
- Name and organization of person visited.

Designated officials within the organization review the visitor access records [Assignment: organization-defined frequency. The organization employs automated mechanisms to facilitate the maintenance and review of access records.

***SA-10 Developer Configuration Management**

The organization requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

***SI-5(1) Security Alerts and Advisories**

The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response. The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

APPENDIX IX: SUPPLEMENTAL CONTROLS FOR INTEGRITY AND AVAILABILITY

APPENDIX X: MAPPING TABLES

NSS #	Control Name	NIST	NISPOM
AU-2	Auditable Events	AU-2	8-602.a
AU-3	Audit Record Contents	AU-3	8-602.a(1)(a)
AU-4	Profile Based Anomaly Detection	N/A	N/A
AU-5	Complex Attack Heuristics	SI-3	8-305
AU-6	Audit Review	AU-7	8-602-d.(1)
AU-7	Audit Data Availability	AU-9	8-6034.b
AU-7(1)	Audit Data Availability	AU-5	N/A
CM-1	Configuration Management System	N/A	8-311.a
CM-2	Configuration Management Documentation	PL-2	8-311, 8-610
DO-1	Delivery Procedures	N/A	10-404
DP-1	Complete Access Control	N/A	N/A
DP-2	Security Attribute Based Access Control	SI-9	N/A
DP-2 (cont)	Security Attribute Based Access Control	N/A	N/A
DP-6	Subset Information Flow Control	AC-4	N/A
DP-7	Simple Security Attributes	N/A	N/A

APPENDIX X: MAPPING TABLES

NSS #	Control Name	NIST	NISPOM
DP-9	Import of User Data w/o Security Attributes	N/A	N/A
DP-11	Full Residual Information Protection	SC-4	8-301.a
DP-12	Stored Data Integrity Monitoring and Action	CP-9	8-604
DV-1	Correspond. Demonstration	SA-5(1)	N/A
EN-1	Malicious Access	SI-4	N/A
EN-2	Management of User Identifiers and Authenticators	IA-5	8-303.f
EN-3	Information Availability	CP-9	8-603
EN-4	Purging	MP-6	8-301.b
EN-6	Hardware and Software Examination	CM-4	8-302
EN-7	Forensics	IR-4	N/A
EN-10	Marking	N/A	N/A
EN-12	User Notification	AC-8	8-609(1)
EN-13	Need-to-Know	N/A	N/A
EN-14	Physical Security	PE-3	8-308.d
EN-15	Physical Access Protection	PE-3(1)	N/A

APPENDIX X: MAPPING TABLES

NSS #	Control Name	NIST	NISPOM
EN-19	Media and Component Review	N/A	8-310.b
EN-23	User Training	AT-2	N/A
EN-24	User Clearance	N/A	8-303.d
EN-24(1)	User Clearance	N/A	N/A
EN-24(2)	User Clearance	N/A	N/A
EN-25	National Security Systems Workstations	N/A	N/A
GD-1	Administrator Guidance	SA-5	N/A
GD-2	User Guidance	SA-5	N/A
IA-1	Authentication Failure Handling	AC-7	8-609(2)
IA-10	User-Subject DAC Binding	N/A	N/A
IA-2	User Attribute Definition	N/A	N/A
IA-4	Timing of Authentication	N/A	N/A
IA-6	Re-authentication	AC-11	N/A
IA-7	Protected Authentication Feedback	IA-6	N/A
IA-8	Timing of Identification	AC-14	N/A

APPENDIX X: MAPPING TABLES

NSS #	Control Name	NIST	NISPOM
IA-9	User Identification Before Any Action	IA-2	8- 302.b, 8-607
LC-1	Identification of Security Measures	PL-2	N/A
LC-2	Flaw Remediation	SI-2	N/A
LC-2(1)	Flaw Remediation	N/A	N/A
LC-2a	Flaw Remediation	SI-2 (1)	N/A
LC-3	Defined Life Cycle Model	SA-3	N/A
MT-1	Management of Security Functions Behavior	CM-3	N/A
MT-2	Management of Security Attributes	AC-3(1)	N/A
MT-3	Static Attribute Initialization	CM-7	N/A
MT-4	Management of Security Data	AU-9	N/A
MT-4(1)	Management of Security Data	N/A	N/A
MT-5	Revocation	N/A	N/A
MT-6	Restriction on Security Roles	IA-4	N/A
PT-1	Information System Security Control Testing	SI-6	N/A
PT-3	Information system Recovery	CP-10	8-612

APPENDIX X: MAPPING TABLES

NSS #	Control Name	NIST	NISPOM
PT-5	Non-bypassability of the Security Policy	N/A	N/A
PT-6	Domain Separation	SC-3	N/A
PT-7	Reliable Time Stamps	AU-8	N/A
PT-8	Fail Secure	CP-10	N/A
SA-2	Session Locking and Termination	AC-11, AC-12	N/A
SA-3	Default Access Banners	AC-8	8-609(1)
SA-4	Information System Access History	AC-9	N/A
TE-1	Test Coverage	NIST 800-53	8-104-J
TE-1(1)	Test Coverage	NIST 800-37	8-201
TE-2	Testing	NIST 800-37	8-201
TE-2(1)	Testing	NIST 800-37	8-201
VA-1	Vulnerability Analysis	RA-5	N/A
VA-1(1)	Vulnerability Analysis	NIST 800-37	N/A
VA-2	Examination of Guidance	NIST 800-371	N/A
VA-2(1)	Examination of Guidance	NIST 800-37	N/A

APPENDIX X: MAPPING TABLES

NSS #	Control Name	NIST	NISPOM
IA-3	Verification of Secrets	N/A	N/A
IA-5	Multiple Authentication Mechanisms	IA-2(1),(2)	N/A
AU-1	Security Alarms	N/A	N/A
AU-3(2)	Audit Record Contents	AU-8	N/A
AU-4(1)	Profile Based Anomaly Detection	AU-6	N/A
CS-1	Crypto Key Establishment and Management	SC-12	N/A
CS-2	Crypto Operation	SC-13	N/A
DP-3	Basic Data Authentication	N/A	N/A
EN-11	Interconnected Environment	PS-6	N/A
EN-16	Environmental Protection	PE-12, PE-14	N/A
EN-17	Information Protection	MP-2	8-605
EN-18	System Recovery	N/A	N/A
EN-8	Intrusion Detection	SC-7	N/A
PT-4	Replay Detection	N/A	N/A
SA-1	Concurrent Session Limitations	AC-10	N/A

APPENDIX X: MAPPING TABLES

NSS #	Control Name	NIST	NISPOM
EN-9	Information System Interface	SC-7(1) (2) (5) (6)	N/A
PT-2	Information System Security Control Data Transmission	SC-9	N/A
TP-1	Trusted Path	SC-11	N/A
AU-2(1)	Auditable Events	N/A	N/A
AU-3(1)	Audit Record Contents	N/A	8-602.a(1)(c)
AU-6(1)	Audit Review	N/A	8-602-c.(1)
CM-1(1)	Configuration Management System	CA-4	8-311.d
CM-2(1)	Configuration Management Documentation	N/A	8-311.d(1)
CO-1	Proof of Origin	AU-10	N/A
CO-2	Proof of Receipt	AU-10	N/A
DO-2	Installation, Generation and Startup Procedures	CA-4, CA-6	8-703
DP-10	Import of User Data with Security Attributes	N/A	N/A
DP-11(1)	Full Residual Information Protection	N/A	N/A
DP-4	Export of User Data w/o Security Attributes	N/A	N/A
DP-5	Export of User Data with Security Attributes	N/A	N/A

APPENDIX X: MAPPING TABLES

NSS #	Control Name	NIST	NISPOM
DP-6(1)	Subset Information Flow Control	N/A	N/A
DP-8	Hierarchical Security Attributes	N/A	N/A
DP-9(1)	Import of User Data w/o Security Attributes	N/A	N/A
DV-1(1)	Correspond. Demonstration	N/A	N/A
DV-2	Implementation of the information System Controls	NIST 800-37	N/A
DV-3	Information System Security Policy Model	N/A	N/A
EN-5	Covert Channels	N/A	N/A
EN-6(1)	Hardware and Software Examination	N/A	8-302.a, 8-302.b
EN-6(2)	Hardware and Software Examination	N/A	N/A
IA-11	User-Subject MAC Binding	N/A	N/A
IA-2(1)	User Attribute Definition	N/A	N/A
MT-2(1)	Management of Security Attributes	N/A	N/A
MT-3(1)	Static Attribute Initialization	N/A	N/A
MT-5(1)	Revocation	N/A	N/A
MT-6(1)	Restriction on Security Roles	N/A	N/A

APPENDIX X: MAPPING TABLES

NSS #	Control Name	NIST	NISPOM
SA-5	Deny Session Establishment	N/A	N/A
PT-2(1)	Information System Security Control Data Transmission	SC-9(1)	N/A
PT-6(1)	Domain Separation	N/A	N/A
RU-1	Quotas	N/A	N/A
RU-1(1)	Quotas	N/A	N/A
EN-20	User Access Right and Privileges	AC-6	N/A
EN-21	Security Roles	AC-5	N/A
EN-22	Two-Person Rule	N/A	N/A

APPENDIX XI: SECURITY PLAN TEMPLATES

The following Security Plan Templates are intended as a guide for sites to utilize to document their NSS program implementation. The following pages contain a sample Site-level NSS Cyber Security Program Plan, and a Site System Security Plan.

[SITE] NATIONAL SECURITY SYSTEMS

CYBER SECURITY PROGRAM PLAN

[VERSION}

[DATE]

TABLE OF CONTENTS

INTRODUCTION 4

1.1 [SITE] MISSION AND OPERATIONAL ENVIRONMENT 4

1.2 SYSTEM IDENTIFICATION AND CATEGORIZATION 4

1.3 SYSTEM POINTS OF CONTACT 4

1.4 PHYSICAL ENVIRONMENT 5

CHAPTER TWO: PROGRAM CHARACTERIZATION 5

2.1 PROGRAM DESCRIPTION 5

2.2 THREAT AND RISK 5

2.3 ORGANIZATIONAL RESPONSIBILITIES 5

2.4 PROGRAM ALIGNMENT 6

CHAPTER THREE: [Acr] NS PROGRAM OVERVIEW 6

3.1 ACCESS REQUIREMENTS 7

3.2 CONFIGURATION MANAGEMENT 7

3.3 TRAINING AND AWARENESS 7

3.4 INFORMATION MARKING 7

3.5 NS INFORMATION STORAGE AND TRANSPORT 8

3.6 VISITOR ACCESS REQUIREMENTS 8

3.7 INTERCONNECTED SYSTEMS 8

3.8 NSS SECURITY PROGRAM COORDINATION 8

3.9 INCIDENT HANDLING AND RESPONSE 9

3.10 CLEARING, PURGING, AND DESTRUCTION 9

3.11 SYSTEM SECURITY PLANS 9

3.12 CERTIFICATION AND ACCREDITATION 10

3.13 METRICS 10
CHAPTER FOUR: NSS CONTROL FAMILIES 10
4.1 SECURITY AUDIT CONTROLS 10
4.2 COMMUNICATION CONTROLS 10
4.3 CRYPTOGRAPHIC SUPPORT CONTROLS 10
4.4 USER DATA PROTECTION CONTROLS 10
4.5 IDENTIFICATION AND AUTHENTICATION CONTROLS 10
4.6 SECURITY MANAGEMENT CONTROLS 11
4.7 PROTECTION OF INFORMATION SYSTEM SECURITY CONTROLS 11
4.8 RESOURCE UTILIZATION CONTROLS 11
4.9 SYSTEM ACCESS CONTROLS 11
4.10 TRUSTED PATH CONTROLS 11
4.11 OPERATIONAL CONTROLS 11
4.12 CONFIGURATION MANAGEMENT CONTROLS 11
4.13 DELIVERY AND OPERATIONS CONTROLS 11
4.14 DEVELOPMENT CONTROLS 12
4.15 GUIDANCE DOCUMENTS CONTROLS 12
4.16 LIFE CYCLE SUPPORT CONTROLS 12
4.17 TEST CONTROLS 12
4.18 VULNERABILITY ASSESSMENT CONTROLS 12
APPENDIX I: REFERENCES I-13
TAPPENDIX II: [Site] RISK AND THREAT ASSESSMENT II-1
APPENDIX III: [SITE] ADDITIONAL DOCUMENTATION III-1

INTRODUCTION

This document outlines the National Security System (NSS) Cyber Security Program Plan for [Site] ([Acr]). It describes the technical, operational and management controls implemented to secure the National Security (NS) systems housed and hosted at [Acr], and represents an approach to securing [Acr] classified cyber assets based on compliance with Federal and DOE policy; the consequence of loss (CoL) for confidentiality, integrity, and availability; and the sensitivity of the information based on classification level, category, and need-to-know.

1.1 [SITE] MISSION AND OPERATIONAL ENVIRONMENT

[Site]'s mission is to [site mission statement, include tie-in to classified program as relevant to the mission of the site and contract number(s)]. The NS systems located at [Acr] are considered [major app/GSS] and support the operational needs of the site and [any other entities]. The [Acr] NS program consists of [describe site-specific operation in general terms, e.g., standalone, mixed environment, etc.].

1.2 SYSTEM IDENTIFICATION AND CATEGORIZATION

The following system(s) are in place at [Acr] and are covered under this Plan:

System Name	Connectivity	Operational Status	Protection Level

1.3 SYSTEM POINTS OF CONTACT

The following are the primary points of contact (POCs) for NS systems at [Acr]:

Function	Organizational POC	E-Mail Address	Phone
Designated Approving Authority			
ISSM			
ISSO			
System Owner – [Program/System]			

[Add all System Owners at site to list.]

1.4 PHYSICAL ENVIRONMENT

[Describe site physical environment, including physical access procedures and controls, storage capability and procedures, classified conferencing capability, classified matter protection and control procedures and controls, etc.]

CHAPTER TWO: PROGRAM CHARACTERIZATION

This chapter describes the systems in place at [Acr] and considers the unique threats there. It integrates these concerns with site operations to identify, evaluate, and integrate the impact of information loss, system vulnerabilities, data custodian protection requirements, cost of protective measures, and mission requirements. It ensures compliance with Federal and DOE policy, and system operation where the remaining risk (residual risk) is accepted and oversight is initiated to ensure that the level of residual risk is managed throughout the information system's life cycle.

2.1 PROGRAM DESCRIPTION

The [Acr].NS program includes [provide a general description of the program and systems in place at the site.]

2.2 THREAT AND RISK

A threat and risk assessment was completed for the site and is attached as Appendix II. This assessment documents the unique threats and risk to the site, and is supplemental to the DOE Threat and Risk Statement. The threat and risk analysis was used to determine the level of protection required for the information processed at [Acr], and augment the NSS protection profiles applied to classified information systems at the site. This analysis is reviewed and updated by the ISSM at least annually.

2.3 ORGANIZATIONAL RESPONSIBILITIES

The following are the primary roles and responsibilities with regard to National Security Systems at [Acr].

- Designated Approving Authority (DAA) – The DAA is a federal employee appointed by the SC Chief Information Officer (CIO). The DAA is responsible for issuing the accreditation and authority to operate after reviewing:
  - The protection measures in an information system as described in the National Security Systems (NSS) Security Plan (SP),
  - The results of any certification tests,
  - The certification of the system, and
  - And any residual risks of operating the system.
- Information Systems Security Site Manager (ISSM) – The ISSM is appointed by the Laboratory Directors to be responsible for implementation of the [Acr] NSS Security Program.
- Information Systems Security Officer (ISSO) – The ISSO is appointed, in writing, by the ISSM and System Owner and ensures implementation of security measures for each classified information system for which he/she is responsible.
- NSS Application Owner/Data Custodian – Determines and declares the sensitivity level of information prior to the information being processed, stored, transferred, or accessed on the classified information system and advises the ISSO of any special protection requirements for information to be processed on the classified information system.
- NSS Users – Comply with all NSS Security Program requirements at [Acr].

2.4 PROGRAM ALIGNMENT

The [Acr] NS Program is aligned with all applicable Federal and DOE requirements, and with the DOE Office of Science Program Cyber Security Plan.

CHAPTER THREE: [ACR] NS PROGRAM OVERVIEW

[Acr] ensures that cyber security controls relevant to classified systems continue to work as intended, that the trust level of classified systems is maintained, and that all changes to cyber security environment are properly recorded and analyzed for impact to the organization and its mission.

All NS systems and information at [Acr] are protected as stated in the attached [Acr] Common Control document and in Chapter Four of this Plan. The systems and information in place at [Acr] are protected at the highest level of sensitivity contained in

the document and system. The controls listed for each PL are mandatory for all systems within that PL at [Acr]. Additional controls, if required due to a higher risk categorization or CoL, are documented in the [Acr] Common Control document and within an approved system SP.

3.1 ACCESS REQUIREMENTS

All personnel must meet all requirements outlined in DOE M 470.4-4, *Information Security* and DOE M 470.4-5, *Personnel Security* prior to being granted access to NS systems and/or information at [Acr]. Procedures for acquiring access to NS systems or information at [Acr] are documented [insert location of procedures. If not separate from this document, insert procedures here].

3.2 CONFIGURATION MANAGEMENT

All NSS systems must be under configuration control and managed according to the controls outlined in this plan. Security-significant changes to the documented configuration of a system immediately nullify its current Authority To Operate. These changes must be documented and the system will need to be re-accredited by the ISSM and DAA before transaction processing may resume.

3.3 TRAINING AND AWARENESS

[Acr] provides a comprehensive training program and awareness briefings and activities for site NSS program management personnel, information security personnel, system administrators, data custodians, users, and escorts in NSS operational areas. Training must be completed prior to being issued authentication credentials for system access, and refreshed yearly thereafter. All users must sign an acknowledgement signifying their understanding of their responsibilities (Code of Conduct) for protecting classified information systems and classified information. The following training and awareness activities are in place at [Acr]:

- [List established training and awareness activities]

The [Acr] training program meets all requirements outlined in DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, Sections J and K.

3.4 INFORMATION MARKING

Classified information and systems at [Acr] are marked at the highest level of sensitivity contained in the document and system and in accordance with DOE M 470.4-4,

Information Security. The procedures for NS information marking are located [insert location of procedures. If not separate from this document, insert procedures here].

3.5 NS INFORMATION STORAGE AND TRANSPORT

All classified information (electronic and hard copy) stored on site or transported between sites is protected as outlined in the controls stated in the [Acr] Common Controls document and Chapter Four of this Plan, and stored in accordance with DOE M 470.4-4, *Information Security* and in DOE M 470.4-2, *Physical Protection.* The procedures for NS information storage and transport are located [insert location of procedures. If not separate from this document, insert procedures here].

3.6 VISITOR ACCESS REQUIREMENTS

Strict physical access control procedures are in place at [Acr] where NS processing, storage, or transmission takes place. All users are trained in the requirements for allowing visitors into area where this information resides. Visitor control requirements are outlined in [insert location of procedures. If not separate from this document, insert procedures here]. These procedures are in accordance with DOE M 470.4-4, *Information Security*, DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*, DOE O 142.1, *Classified Visits Involving Foreign Nationals,* and TMR 16, *Foreign National Access to DOE Information Systems*.

3.7 INTERCONNECTED SYSTEMS

NS system interconnection policies and procedures at [Acr] are consistent with TMR 5, *Interconnected Systems Management,* and are commensurate with the level of security required for [Acr]'s environment and program-specific needs. The procedures for interconnected systems at [Acr] are located [insert location of procedures. If not separate from this document, insert procedures here]. Appendix III contains the standard Memorandum of Understanding/Memorandum of Agreement (MOU/MOA) utilized at [Acr].

All interconnections are approved as part of the system certification and accreditation by the cognizant DAA for each interconnected party.

3.8 NSS SECURITY PROGRAM COORDINATION

The NSS Security Program at [Acr] ensures that the program is coordinated with other site programs governing classified information, as appropriate, such as Information Security, Personnel Security, Physical Security, Communications Security, Protected

Transmission Systems, TEMPEST, and Materials Control and Accountability. The procedures for assuring program coordination are located [insert location of procedures. If not separate from this document, insert procedures here].

3.9 INCIDENT HANDLING AND RESPONSE

[Acr] maintains a rigorous Cyber Incident Response program for classified information, which includes the establishment of a Cyber Incident Response Team (CIRT) that is trained in proper incident handling procedures. The procedures for incident handling and response at [Acr] are located [insert location of procedures. If not separate from this document, insert procedures here].

The program includes all required elements outlined in TMR 9, *Incident Management Guidance*, as well as the procedures outlined in Attachment 2, Part II, Section N, Chapter II, *Incidents of Security Concern Involving Compromise or Potential Compromise of Classified Information* of DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.

3.10 CLEARING, PURGING, AND DESTRUCTION

[Acr] has developed, documented, and implemented processes for the clearing, purging, and destruction of classified media, storage devices, and other hardware utilizing the applicable criteria in TMR 10, *Media Clearing, Purging and Destruction* and commensurate with the level of security required for the [Acr]'s environment and specific needs. The procedures for clearing, purging, and destroying classified media, storage devices, and other hardware are located [insert location of procedures. If not separate from this document, insert procedures here].

The requirements for removing information from storage media, memory devices, and related hardware are reviewed with all users on a regular basis. Personnel performing or verifying the clearing, purging, or destruction of storage media, memory devices, and other hardware are trained in equipment/tool operation, approved techniques, and procedures.

3.11 SYSTEM SECURITY PLANS

All systems storing, processing, or transmitting NS information at [Acr] comply with this Plan. In addition, system specific information and controls are supported by an approved system security plan (SSP), which is maintained by the ISSM. All security plans at [Acr] are reviewed and approved every three years, or when a security significant change occurs.

3.12 CERTIFICATION AND ACCREDITATION

All NSS systems at [Acr] are certified and accredited prior to being placed in use in accordance with TMR 2, *Certification and Accreditation*.

3.13 METRICS

[Acr] maintains metrics documentation and reporting for the following:

- [List metrics maintained on- site]

The current POA&Ms for [Acr] are located [list location].

CHAPTER FOUR: NSS CONTROL FAMILIES

This section outlines the controls in place at [Acr] to address each of the 18 control families under the three control classes (Technical, Operational, and Assurance).

4.1 SECURITY AUDIT CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.2 COMMUNICATION CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.3 CRYPTOGRAPHIC SUPPORT CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.4 USER DATA PROTECTION CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.5 IDENTIFICATION AND AUTHENTICATION CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.6 SECURITY MANAGEMENT CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.7 PROTECTION OF INFORMATION SYSTEM SECURITY CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.8 RESOURCE UTILIZATION CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.9 SYSTEM ACCESS CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.10 TRUSTED PATH CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.11 OPERATIONAL CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.12 CONFIGURATION MANAGEMENT CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.13 DELIVERY AND OPERATIONS CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.14 DEVELOPMENT CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.15 GUIDANCE DOCUMENTS CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.16 LIFE CYCLE SUPPORT CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.17 TEST CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

4.18 VULNERABILITY ASSESSMENT CONTROLS

[Insert a description and/or references of how the site meets the requirements for these controls.]

APPENDIX I: REFERENCES

DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 4, 5

DOE M 470.4-2, *Physical Protection*, 4

DOE M 470.4-5, *Personnel Security*, 3

DOE O 142.1, *Classified Visits Involving Foreign Nationals*, 4

DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*, 4

DOE Office of Science Program Cyber Security Plan, 3

DOE Threat and Risk Statement, 2

TMR 10, *Media Clearing, Purging and Destruction*, 5

TMR 16, *Foreign National Access to DOE Information Systems*, 4

TMR 2, *Certification and Accreditation*, 6

TMR 5, *Interconnected Systems Management*, 5

TMR 9, *Incident Management Guidance*, 5

APPENDIX II: [SITE] RISK AND THREAT ASSESSMENT

Insert site-specific Threat and Risk Assessment here.

APPENDIX III: [SITE] ADDITIONAL DOCUMENTATION

Insert additional site information if available and applicable to support Master Plan. This may include network diagrams, references to site-specific plans and procedures, MOU/MOAs, if used, or other documentation pertinent to the security of NSS systems at SC sites.

APPENDIX IV: [SYSTEM] SYSTEM SECURITY PLAN

Insert additional system information for those systems that requires controls beyond those listed in the Site Security Plan (Master Plan). These would include periods processing, isolated network, and networked systems.

SYSTEM IDENTIFICATION AND CATEGORIZATION

System Location	LSA	VTR	Conf. Rm.	Diskless Terminal

System Name/Number	Connectivity	Operational Status	Protection Level

SYSTEM POINTS OF CONTACT

Function	Name	Clearance Level	Training Completion Date
System Owner			
ISSO			
Alternate ISSO			
System Administrator			
User			

A signed User Agreement, and signed System Administrator Code of Conduct for all individuals with privileged access, **must** be attached for all personnel with access credentials to this system.

SYSTEM CHARACTERIZATION

Component and Software Inventory

Description	Serial Number (if applicable)	Other Information (i.e., Property Number, Specialized Software, etc.)

General Information

Location of audit records	
Location of configuration management documentation and records	
Location of system and software documentation	
Backup schedule and storage location	
Method for controlling creation of CREM/ACREM	

Variance from Master Security Plan

If *any* controls on this system vary from the [Site] NSS Cyber Security Program Plan, all controls, mitigating controls, and rationale should be documented below. This should include supplemental controls implemented for availability and integrity concerns.

Control	Mitigation	Rationale

Test/Inspection Dates and Results

Test/Inspection Date	Results	POA&M Actions

Certification Approvals

_____ _____

[Name] Date

System Owner/Program Manager

[Name]
Information System Security Officer

Date

[Name]
Information System Security Manager

Date

System Retirement

Date of Retirement	Method of Disposition

[Name]
Information System Security Manager

Date

APPENDIX XII: SAMPLE MOU/MOA

The following pages contain a sample MOU/MOA which can be used as a template for SC sites. MOU/MOAs should be reviewed by site legal counsel prior to being placed in use.

APPENDIX XII: SAMPLE MOU/MOA

MEMORANDUM OF UNDERSTANDING/MEMORANDUM OF AGREEMENT

BETWEEN

[SITE]

AND

[SPONSORING PROGRAM OR ENTITY]

This Memorandum of Understanding/Memorandum of Agreement (MOU/MOA) between [Site] and [Sponsoring Program or Entity] is for the purpose of establishing a trusted communications link between [Site] and [Sponsoring Program or Entity] for the electronic transfer of information. Each of the undersigned agrees to and understands the procedures that will be in effect and adhered to. It is also understood that this MOU/MOA summarizes the information system (IS) security requirements for approval purposes and supplements the [Site] and [Sponsoring Program or Entity]'s approved system security plan (SSP).

1. Contract Information

This MOU/MOA describes the network arrangement between [Site] and [Sponsoring Program or Entity] in support of the [Name of Program]. The [Name of Program] is a [brief description of program] sponsored by [Agency]. The contract number is [Contract Number]. The prime contractor is [Name of Prime Contractor].

The following key points of contact are identified:

[Site]

Function	Organizational POC	E-Mail Address	Phone
Designated Approving Authority			
ISSM			
System			

APPENDIX XII: SAMPLE MOU/MOA

Function	Organizational POC	E-Mail Address	Phone
Owner/Program Manager			

[Sponsoring Program or Entity]

Function	Organizational POC	E-Mail Address	Phone
Designated Approving Authority			
ISSM			
System Owner/Program Manager			

2. Description

At [Sponsoring Program or Entity]'s direction, [Site] is establishing an access capability to the [Name of Computer System] located at [Processing Location]. *(Note to Template User: Please word this paragraph so that it is obvious who will be the host, if applicable, and who will be the remote computer system).* This capability will allow [Site] personnel to access the [Name of Computer System] as remote users.

[Site] operates the [Name of Computer System] at [insert protection level of control], whereby all users have the need to know for all information on the system.

The [Sponsoring Program or Entity] will be connected to the [Site] [Name of Computer System] at [Processing Location], by [Describe connection] communications circuit for the transfer of data via a [describe type of network]. The circuit will be protected at each end by [describe protection mechanisms/devices that provides the required level of security. Include network diagrams and descriptions, as appropriate. Describe site-level responsibilities and protections required to maintain the interconnection, with appropriate responsibilities (Site or Sponsoring Program or Entity) clearly outlined].

3. Information System Security Officer Responsibilities

APPENDIX XII: SAMPLE MOU/MOA

The Information System Security Officer (ISSO) at [Site} will [outline specific responsibilities with regard to the interconnection. Include or reference procedures, if applicable.].

The ISSO at [Site] will brief operator personnel involved with use of communications and network operating procedures and their responsibilities for safeguarding information in accordance with the requirements of the CSPP. The ISSO at [Sponsoring Program or Entity] will conduct an equivalent briefing for information system responsible personnel.

These briefings will include:

a. The need for sound security practices for protecting information handled by their respective IS, including all input, storage, and output products.
b. The specific security requirements associated with their respective IS as they relate to CSPP controls and operator access requirements.
c. The security reporting requirements and procedures in the event of a system malfunction or other security incident.
d. What constitutes an unauthorized action as it relates to system usage.
e. Their responsibility to report any known or suspected security violations.

It is the responsibility of each individual operator to understand and comply with all required procedures for using the systems at each site, as described in their respective system security plans.

4. Approval

The communication link between [Site] and [Sponsoring Program or Entity] shall not be initialized until approval of these procedures by the DAA is indicated below.

[Name] Designated Approving Authority – [Site]	Date

APPENDIX XII: SAMPLE MOU/MOA

[Name] Information System Security Manager – [Site]	Date
[Name] System Owner/Program Manager – [Site]	Date
[Name] Designated Approving Authority – [Sponsoring Program or Entity]	Date
[Name] Information System Security Manager – [Sponsoring Program or Entity]	Date
[Name] System Owner/Program Manager – [Sponsoring Program or Entity]	Date

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

Minor verbiage changes were made to the NSS controls in order to provide Office of Science sites with clarity on the intent of the control, or controls were added where SC exercised a higher level of due diligence than the original controls. The following outlines the control description comparisons between this Manual and the original NSS Manual text. The original NSS verbiage is listed first in *italics*, and if modifications were made by the Office of Science, the new verbiage is printed under it with the changes highlighted in **bold**. Only modified controls are listed.

AU-4 Profile Based Anomaly Detection

The information system security controls shall be able to maintain profiles of systems usage, where an individual profile represents the historical patterns of usage performed by single users and/or members of group accounts and/or [profile target group(s) (e.g. users who share a group ID or group account, users who operate under an assigned role, users of an entire system or network node)].

The audit log provides the capability to determine the historical usage of system resources by individual

AU-5 Complex Attack Heuristics

The information system security controls shall maintain an internal representation of the event sequences of known intrusion scenarios and signature events that may indicate a potential violation of information system security; compare the signature events and event sequences against a record of system activity; and alert security personnel (e.g., system owner, Alternate ISSO, network administrator)] of a potential imminent violation of information system security when system activity is found to match a signature event or event sequence that indicates a potential violation of information system security.

Anti virus software is installed and operational on standalone systems and Intrusion Detection Software (IDS) is installed and operational for networked systems. The IDS will alert security personnel (e.g., system owner, Alternate ISSO, network administrator)] of a potential imminent violation of information system security when system activity is found to match a signature event or event sequence that indicates a potential violation of information system security.

AU-6 Audit Review

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

The information system security controls shall provide the ISSO and authorized system administrators with the audit records and the capability to read all audit information from the audit records in a manner suitable for interpreting the information. Read access to the audit records shall be prohibited to all other users. The information system security controls shall provide the ability to perform searches, sorting, and ordering of audit data based on user identity. Audit records shall be reviewed at least weekly and retained for at least one year.

The system has a mechanism to extract relevant information based on user identification. Network systems checked weekly; standalone systems as part of a forensics investigation. Read access to the audit records shall be prohibited to all users **except the ISSO and authorized system administrators.** The information system security controls shall provide the ability to perform searches, sorting, and ordering of audit data based on user identity.

AU-7 Audit Data Availability

The stored audit records shall be protected from unauthorized deletion, prevent modification, and ensure that records already written (i.e. to media) will be maintained when the audit storage is exhausted, the system fails, or an attack occurs. An alarm (e.g. any clear indication that the pre-defined limit has been exceeded) shall be generated and provided to the ISSO and the authorized system administrator if the audit trail storage exceeds 80% of capacity. The information system shall prevent auditable events from being lost (e.g., deleted, overwritten, not recorded), except those taken by the ISSO or authorized system administrator if the audit trail has reached storage capacity.

The stored audit records shall be protected from unauthorized deletion, prevent modification, and ensure that records already written (i.e. to media) will be maintained when the audit storage is exhausted, the system fails, or an attack occurs. An alarm (e.g. any clear indication that the pre-defined limit has been exceeded) shall be generated and provided to the ISSO and the authorized system administrator if the audit trail storage exceeds 80% of capacity **on networked systems. For standalone systems the user will not be able to process work. The information system shall prevent auditable events from being lost (e.g., deleted, overwritten, not recorded),** except those taken by the ISSO or authorized system administrator if the audit trail has reached storage capacity.

CM-2 Configuration Management Documentation

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

Documentation shall show that the CM system, as a minimum, tracks the following: The information system implementation representation, design documentation, functional and security test documentation, user documentation, administrator documentation, and CM documentation (e.g., version and change log). The CM documentation shall describe how the configuration items are tracked by the CM system.

The certifier, during the C&A process, shall confirm that the documentation provided meets all the requirements for the content.

The organization authorizes, documents, and controls changes to the information system. The organization : (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.

The certifier, during the C&A process, shall confirm that the documentation provided meets all the requirements for the content.

***CM-5(1) Access Restrictions for Change**

The organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes. The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

***CM-8(2) Information System Component Inventory**

The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information. The organization employs mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

DO-1 Delivery Procedures

The system owner shall document procedures for delivery of the information system or parts of it to the user and shall use the delivery procedures. The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the information system or updates to the user's site.

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

The certifier, during the C&A process, shall confirm that the documentation provided meets all the requirements for the content.

The **ISSO** shall document procedures for delivery of the information system or parts of it to the user and shall use the delivery procedures. The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the information system or updates to the user's site.

The certifier, during the C&A process, shall confirm that the documentation provided meets all the requirements for the content.

DP-1 Complete Access Control

The information system security controls shall enforce the Discretionary Access Control (DAC) security policy based on access authorization and need-to-know on all subjects acting on behalf of users, all named objects, and all operations among subjects and objects covered by the DAC security policy. The DAC security policy shall apply to all operations between any object and subject within the information system. Any named object that is not controlled by the DAC security policy must be justified in the SSP.

The information system **implements the access controls correctly for all users (subjects) of the system, including read, write, create, update, and delete for the databases/files (objects) within the system.** The DAC security policy shall apply to all operations between any object and subject within the information system. Any named object that is not controlled by the DAC security policy must be justified in the SSP.

DP-2 Security Attribute Based Access Control

The information system security controls shall enforce the DAC security policy to objects based on the user identity and group memberships associated with a subject; and the following access control attributes associated with an object: [list access control attributes (e.g., identity of users, subjects, or objects; time restrictions; group membership)]. The access control attributes must provide the ability to associate allowed or denied operations with one or more user identities; the ability to associate allowed or denied operations with one or more group identities; and defaults for allowed or denied operation The DAC defines "subject" as users or user groups, and "objects" as file servers, database, print servers, etc, and shall enforce the security policy based on group membership associated with a subject.

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

In addition to the rules specified in DP-1, the information system security controls shall enforce [a set of rules specifying the DAC policy] to determine if an operation among controlled subjects and controlled objects is allowed. For each operation, there shall be a DAC rule, or rules, that use:

- *The permission attributes where the user identity of the subject matches a user identity specified in the access control attributes of the object;*
- *The permission attributes where the group membership of the subject matches a group identity specified in the access control attributes of the object; and*
- *The default permission attributes specified in the access control attributes of the object when neither a user identity nor group identity matches.*

The information system security controls shall explicitly authorize or deny access of subjects to objects based on the [rules, based on security attributes, which explicitly authorize or deny access of subjects to objects (e.g., a specific privilege vector associated with a subject that always grants or denies access to specific objects)].In completing the rules above, the resulting mechanism must be able to specify access rules that apply to at least any single user. The mechanism must also support specifying access to the membership of at least any single group. Specification of these rules must be covered under DP-2 and DP-3. The PCSP or SSP must list the attributes that are used by the DAC policy for access decisions.

The DAC is implemented to assure that everyone (subjects) is not entitled to have all access to all resources (objects).

DP-6 Subset Information Flow Control The DAC security policy shall be enforced on [list of subjects (e.g., users, machines, processes), information (e.g., email, files, specified network protocols), and operations that cause controlled information to flow to and from controlled subjects covered by DAC].

All subjects and object are tied either one to one or one to many.

DP-9 Import of User Data w/o Security Attributes

When importing data from outside the control of the information system (via authorized means, such as removable media or document scanner), the information system security controls shall enforce the DAC security policy regardless of the security attributes associated with the data.

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

The Operating System (OS) of the workstation or fileserver will be configured to assure that when importing data from outside the control of the information system (via authorized means, such as removable media or document scanner), the information system security controls shall enforce the DAC security policy regardless of the security attributes associated with the data. **Devices that do not support this function will be isolated from a network via firewall.**

DP-11 Full Residual Information Protection

The information system security controls shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource.

The information system security controls shall ensure that any previous information content of a resource **(e.g. cache, RAM, temp file, cookies, deleted page files)** is made unavailable upon the allocation of the resource.

DP-12 Stored Data Integrity Monitoring and Action

The information system security controls shall monitor user data stored within the control of the information system for unauthorized modification and unauthorized deletion on all objects, based on the following [user data attributes]:

**When storing data to persistent storage, the information system shall make use of the underlying error detection/correction mechanisms of the media, and will detect and report failures on re-read.*

**Where a particular persistent storage device does not innately provide an effective correction facility, the information system shall store data in such a way as to independently compute and validate an appropriate error detection check.*

Upon detection of a data integrity error, the information system security control shall enter a description of the error in the audit log and issue an alarm.

The information system assures that only authorized personnel have access to stored information. The information system security controls shall monitor user data stored within the control of the information system for unauthorized modification and unauthorized deletion on all objects. When storing data to persistent storage, the information system shall make use of the underlying error detection/correction mechanisms of the media, and will detect and report failures on re-read. Where a particular persistent storage device does not provide an effective correction facility, the information system shall store data in such a way as to independently compute and

validate an appropriate error detection check. Upon detection of a data integrity error, the information system security control shall enter a description of the error in the audit log and issue an alarm.

DV-1 Correspond. Demonstration

The system owner shall provide a functional specification for systems other than Commercial Off-the-Shelf (COTS) software. The functional specification shall provide the high-level design. The system owner shall provide the high-level design (HLD) of the information system security controls. The HLD shall be internally consistent; shall describe the structure of the information system security controls in terms of subsystems; shall describe the security functionality provided by each subsystem of the information system security controls; shall identify any underlying hardware, firmware, and / or software required by the information system security controls with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software; shall identify all interfaces to the subsystems of the information system security controls; and shall identify which of the interfaces to the subsystems of the information system security controls are externally visible.

The certifier, during the C&A process, shall confirm that the documentation provided meets all the requirements for content, shall determine that the functional specification is an accurate and complete representation of the information system security functional requirements, and determine that the high-level design is an accurate and complete description of the information system security functional requirements.

The **system developer shall provide the ISSO** a functional specification for systems other than Commercial Off-the-Shelf (COTS) software. The functional specification shall provide the high-level design. The system owner shall provide the high-level design (HLD) of the information system security controls. The HLD shall be internally consistent; shall describe the structure of the information system security controls in terms of subsystems; shall describe the security functionality provided by each subsystem of the information system security controls; shall identify any underlying hardware, firmware, and / or software required by the information system security controls with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software; shall identify all interfaces to the subsystems of the information system security controls; and shall identify which of the interfaces to the subsystems of the information system security controls are externally visible.

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

The certifier, during the C&A process, shall confirm that the documentation provided meets all the requirements for content, shall determine that the functional specification is an accurate and complete representation of the information system security functional requirements, and determine that the high-level design is an accurate and complete description of the information system security functional requirements.

***SA-5(1) Information System Documentation**

The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

***SA-10 Developer Configuration Management**

The organization requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

EN-1 Malicious Access

Information system security controls shall be implemented to detect, deter, and respond to malicious actions by authenticated users.

Information system security controls shall be implemented to detect, deter, and respond to malicious actions by authenticated users. **Malicious actions include installing or use of unauthorized software, attempting to access network resources, change security configurations, etc. as defined in the Code of Conduct.**

EN-3 Information Availability

Capabilities and resources shall be provided to allow the information system user to perform data backup at the user's discretion. User and information system data shall be available, or restorable, to meet mission availability requirements. Periodic checking of backup inventory and testing of the ability to restore information shall be accomplished to validate mission availability requirements are met. The organization shall conduct backups of user-level and system-level

information (including system state information) contained in the information system [Assignment: organization-defined frequency].

Capabilities and resources shall be provided to allow the information system user to perform data backup at the user's discretion. User and information system data shall be available, or restorable, to meet mission availability requirements. Periodic checking of backup inventory and testing of the ability to restore information shall be accomplished to validate mission availability requirements are met. **The organization shall conduct backups of user-level and system-level information (including system state information) contained in the information system. Backups shall be done at least monthly if the information system is used daily.**

EN-6 Hardware & Software Examination

Information system hardware and software components shall be examined for security impacts to the information system before use.

The information system hardware and software shall be examined for security impacts to the information system **upon installation.**

EN-12 User Notification

All users shall be notified that they are subject to being monitored, recorded, and audited through the use of the following approved warning text.:

WARNING**WARNING**WARNING**WARNING** This is a Department of Energy (DOE) computer system. DOE computer systems are provided for the processing of official U.S. Government information only. All data contained within DOE computer systems is owned by the DOE, and may be audited, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DOE computer systems to appropriate authorities. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS AUDITING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, and DISCLOSURE OF COMPUTER ACTIVITY.**WARNING**WARNING**WARNING**WARNING

Explicit acknowledgement of the warning by the user is required before granting the user access to system resources

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

This banner or a banner that conveys the same limitations on privacy shall be presented to the user prior to granting access to system resources. All users shall be notified that they are subject to being monitored, recorded, and audited through the use of the following approved warning text:

WARNINGWARNING**WARNING**WARNING** This is a Department of Energy (DOE) computer system. DOE computer systems are provided for the processing of official U.S. Government information only. All data contained within DOE computer systems is owned by the DOE, and may be audited, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DOE computer systems to appropriate authorities. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS AUDITING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, and DISCLOSURE OF COMPUTER ACTIVITY.**WARNING**WARNING**WARNING**WARNING**

Explicit acknowledgement of the warning by the user is required before granting the user access to system resources

EN-19 Media and Component Review

All media (paper, disks, zip drives, removable disk drives, etc.) shall be reviewed by an authorized derivative classifier for sensitivity and properly marked before release outside the system boundary.

The organization: (i) affixes external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and (ii) exempts from labeling all media so long as they remain within protected environment. All media (paper, disks, zip drives, removable disk drives, etc.) shall be reviewed by an authorized derivative classifier for sensitivity and properly marked before release outside the system boundary.

EN-20 User Access Right and Privileges

Each user's access rights and privileges shall be based on the least privilege principle and authorized by the data owner or user(s) authorized by the ISSO prior to the user's first access to the information system.

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

User must log on with the least privileges to do the job. The data owner defines the need to know and operational requirements for the users. ISSO determines the privileges needed to accomplish the task.

EN-21 Security Roles

The same person must not perform the functions of the ISSO and the system administrator. Other roles involved with security administration, such as DBMS administration, must not performed by the same people performing the ISSO and system administrator roles.

The same person must not perform the functions of **implementing security changes and security approval of said changes.** Other roles involved with security administration, such as DBMS administration, must not performed by the same people performing the change and the approval. **All system administrators must sign and adhere to a Code of Conduct agreement which outlines their responsibilities with regard to being granted privileged access to NSS.**

EN-22 Two-Person Rule

The ISSO and system administrator shall be present when audit parameters or audit file contents are modified

Two security trained & technically knowledgeable people approved by the ISSM or DAA (e.g. ISSO and system administrator) shall be present when audit parameters or audit file contents are modified.

GD-1 Administrator Guidance

The system owner shall provide administrator guidance to system administrative personnel. The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the information system; shall describe how to administer the information system in a secure manner; shall contain warnings about functions and privileges that should be controlled in a secure processing environment; shall describe all assumptions regarding user behavior that are relevant to secure operation of the information system; shall describe all security parameters under the control of the administrator, indicating secure values as appropriate; shall describe each type of security relevant event relative to the administrative function that needs to be performed, including changing the security characteristics of entities under the control of the

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

information system security controls; shall describe and be consistent with all other documentation supplied for evaluation; and shall describe all security requirements for the IT environment that are relevant to the administrator.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

The system owner shall provide the system administrator a system security document that outlines the functional requirements and protections required for the system.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

IA-1 Authentication Failure Handling

The information system security controls shall detect when no more than five (5) consecutive unsuccessful authentication attempts occur related to the last successful session authentication for the indicated user. When the defined number of unsuccessful authentication attempts has been met or surpassed, the information system security controls shall inform the system administrator and disable the user account until it is unlocked by the administrator.

The information system security controls shall detect when no more than **three (3)** consecutive unsuccessful authentication attempts occur related to the last successful session authentication for the indicated user. When the defined number of unsuccessful authentication attempts has been met or surpassed, the information system security controls shall inform the system administrator and disable the user account until it is unlocked by the administrator. **Standalone systems that do not have notification systems should be set to lock user and note in audit log.**

IA-10 User-Subject DAC Binding

The information system security controls shall associate the following user security attributes with subjects acting on behalf of that user: the user identity that is associated with auditable events; the user identity or identities that are used to enforce the DAC security policy; and the group membership or memberships used to enforce the DAC security policy.

The DAC shall establish a set of rules between the users (subjects) and the system resources (objects) with respect to what the uses can do with those objects. (e.g. read,

write, create, delete, edit). The information system shall record user activities in the event logs.

IA-9 User Identification Before Any Action

The information system security controls shall require each user to identify itself before allowing any other information system security controls mediated actions on behalf of that user.

The information system security controls does not allow guest or anonymous users to have access to system resources.

LC-1 Identification of Security Measures

The system owner shall produce development security documentation. The development security documentation shall describe all physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the information system design and implementation in its development environment and shall provide evidence that these security measures are followed during the development and maintenance of the information system.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content and shall confirm that the security measures are being applied.

The **ISSO/ISSM shall produce the program and system security plans. The system security plan** shall describe all physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the information system design and implementation in its development environment and shall provide evidence that these security measures are followed during the development and maintenance of the information system.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content and shall confirm that the security measures are being applied.

LC-2 Flaw Remediation

Flaws in hardware or software may adversely affect the confidentiality, availability, or integrity of national security information. Flaws may be identified through a variety of means, such as vendor notifications, vulnerability analysis, or certification testing. The system owner shall document the flaw remediation procedures. The flaw remediation procedures documentation shall

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

describe the procedures used to track all reported security flaws in each release of the information system and shall describe the methods used to provide flaw information, corrections, and guidance on corrective actions to information system users. The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided as well as the status of finding a correction to the flaw and shall require that corrective actions be identified for each of the security flaws.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

Flaws in **COTS** hardware or software may adversely affect the confidentiality, availability, or integrity of national security information. Flaws may be identified through a variety of means, such as vendor notifications, vulnerability analysis, or certification testing. The system owner shall document the flaw remediation procedures. The flaw remediation procedures documentation shall describe the procedures used to patch operating system and application software vulnerabilities, update virus signature files, or modify the configuration settings of the targeted device. The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided as well as the status of finding a correction to the flaw and shall require that corrective actions be identified for each of the security flaws.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

MT-1 Management of Security Functions Behavior

The information system security controls shall restrict the ability to determine or modify the behavior of, disable, and enable the functions [list of security functions (e.g., management functions that relate to access control, accountability and authentication controls, controls over availability)] to ISSOs and authorized system administrators.

The information system security controls **limit access and changes to the security functions (configuration setting, audit logs, etc)** to ISSOs and authorized systems administrators.

MT-2 Management of Security Attributes

The information system security controls shall enforce the DAC security policy to restrict the ability to modify the security attributes [list of access control attributes (e.g., the groups to which

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

a user belongs and the rights, such as read, write, and execute belonging to a role or user.)]. The information system security controls shall ensure that only SSP-defined values are accepted for security attributes. The PCSP or SSP must state the components of the access rights that may be modified, must state any restrictions that may exist for a type of authorized user, and the components of the access rights that the user is allowed to modify. The ability to modify access rights must be restricted in that a user having access rights to a named object does not have the ability to modify those access rights unless granted the right to do so.

The information system security controls limit access and changes to the Access Control List (ACL) to ISSOs and authorized systems administrators.

MT-3 Static Attribute Initialization

The information system security controls shall enforce the DAC security policy to provide restrictive default values for security attributes that are used to enforce the DAC security policy.

The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: (e.g. peer to peer, anonymous FTP). The organization reviews the information system (if standalone -once every six months), to identify and eliminate unnecessary functions, ports, protocols, and/or services (note: standalone systems may have dial up access capability for diagnostic purposes).

MT-4 Management of Security Data

The information system security controls shall restrict the ability to create, delete, and clear the audit trail and to modify and observe the set of audited events to ISSOs and authorized system administrators. The information system security controls shall restrict the ability to initialize the authentication data and initialize and modify the user security attributes, other than authentication data, to authorized system administrators. The information system security controls shall restrict the ability to modify the authentication data to authorized system administrators and those users explicitly authorized to modify their own authentication data (e.g., passwords).

The information system security controls shall permit only authorized SA and ISSOs to modify (delete/clear) the audit logs, or change other authentication data (e.g. passwords).

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

MT-4(1) Management of Security Data

The information system security controls shall restrict the ability to modify the information system and object representation of time to ISSOs and authorized system administrators.

The information system security controls shall **permit only authorized SA and ISSOs to change the system time.**

MT-5 Revocation

The information system security controls shall restrict the ability to revoke security attributes associated with the users within the information system's control to the ISSO and authorized system administrators. The information system security controls shall enforce the immediate revocation of security-relevant authorizations (e.g., next login, next attempt to open the file, within a fixed time). Upon revocation of security-relevant authorizations (e.g., disable subject) the system must [list of authorized actions (e.g., reassign ownership of objects, disable access to objects)] to ensure control of objects owned by subject. The information system security controls shall restrict the ability to revoke the security attributes associated with objects within the information system's control to users authorized to modify the security attributes by DAC or MAC security policies. The information system security controls shall enforce the access rights associated with an object when an access check is made.

The information system security controls shall **assure only the ISSO and authorized system administrators that can revoke security attributes associated with the users within the information system.** The information system security controls shall enforce the revocation of the attributes **in real time (if a standalone system - upon system reboot).** Upon revocation of security-relevant authorizations (e.g., disable subject) the system must reassign ownership of objects, to approved subjects within the information system. The information system security controls shall enforce the access rights associated with an object when an access check is made.

PT-1 Information System Security Control Testing

The information system controls shall run a suite of self-tests (e.g., hardware page protection, sample communications across a network to ensure receipt, and verifying the behavior of specific controls) during initial start-up, periodically during normal operation, or at the request of the authorized user and [list other conditions under which self test should occur (e.g., recovery from

failed condition/event)] to demonstrate the correct operation of the information system security controls.

The information system controls shall run a suite of self-tests **(e.g., Power-On Self Test)** during initial start-up, periodically during normal operation, or at the request of the authorized user **(e.g., recovery from failed condition/event)** to demonstrate the correct operation of the information system security controls.

PT-5 Non-bypassability of the Security Policy

The information system security controls shall ensure that the information system security policy enforcement functions are invoked and succeed before each function within the information system's control is allowed to proceed.

The information system security controls shall ensure that the information system security policy enforcement functions **(e.g. role based access controls)** are invoked and succeed before each function within the information system's control is allowed to proceed.

PT-6 Domain Separation

The un-isolated portion of the information system security controls shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects and shall enforce separation between the security domains of subjects under the control of the information system. The information system security controls shall maintain the part of the information system security controls related to the DAC security policy in a security domain for their own execution that protects them from interference and tampering by the remainder of the information system's controls and by subjects untrusted with respect to those DAC security policy.

The un-isolated portion of the information system security controls shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects and shall enforce separation between the security domains of subjects under the control of the information system. The information system security controls shall maintain the part of the information system security controls related to the DAC security policy in a security domain for their own execution that protects them from interference and tampering by the remainder of the information system's controls

and by subjects untrusted with respect to those DAC security policy. **If third party software is applied as a security control it is set so that only the administrator may change the software setting.**

TE-1(1) Test Coverage

The system owner shall provide an analysis of test coverage. The analysis of test coverage shall demonstrate the correspondence between the test identified in the test documentation and the information system security controls as described in the functional specification and between the information system security controls as described in the functional specification and the tests identified in the test documentation is complete

The **ISSO** shall provide an analysis of test coverage. The analysis of test coverage shall demonstrate the correspondence between the test identified in the test documentation and the information system security controls as described in the functional specification and between the information system security controls as described in the functional specification and the tests identified in the test documentation is complete. **A gap report and POA&M list will be prepared as evidence of this control, if required.**

TE-2 Testing

The system owner shall test the information system security controls and document the results. The system owner shall provide test documentation that consists of test plans, test procedure descriptions, expected test results, and the actual test results. The test plans shall identify the security controls to be tested and describe the goal of the tests to be performed. The test procedures shall identify the test to be performed and describe the scenarios for testing each security function. The scenarios shall include any ordering dependencies on the results of other tests. The expected test results shall show the anticipated outputs from a successful execution of the tests. The test results from the system owner execution of the tests shall demonstrate that each tested security control behaved as specified. The system owner shall provide a suitable information system for testing and shall provide an equivalent set of resources to those that were used in the system owner's functional testing of the information system security controls.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content, shall select and test a subset of the information system security controls as appropriate to confirm that the information system operates as specified, and shall execute a sample of tests in the test documentation to verify the system owner test results.

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

The **ISSO** shall test the information system security controls and document the results. The system owner shall provide test documentation that consists of test plans, test procedure descriptions, expected test results, and the actual test results. The test plans shall identify the security controls to be tested and describe the goal of the tests to be performed. The test procedures shall identify the test to be performed and describe the scenarios for testing each security function. The scenarios shall include any ordering dependencies on the results of other tests. The expected test results shall show the anticipated outputs from a successful execution of the tests. The test results from the system owner execution of the tests shall demonstrate that each tested security control behaved as specified. The system owner shall provide a suitable information system for testing and shall provide an equivalent set of resources to those that were used in the system owner's functional testing of the information system security controls.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content, shall select and test a subset of the information system security controls as appropriate to confirm that the information system operates as specified, and shall execute a sample of tests in the test documentation to verify the system owner test results.

TE-2(1) Testing

The system owner shall provide the analysis of the depth of testing. The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the information system security controls operates in accordance with its high-level design.

The system owner shall provide the analysis of the depth of testing. The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the information system security controls operates in accordance with its high-level design **(e.g. which controls were tested via interview, observation or functional test)**.

VA-1 Vulnerability Analysis

The system owner shall perform and document an analysis of the information system deliverables searching for obvious ways in which a user can violate the information system security policy. The system owner shall document the disposition of the obvious vulnerabilities and the documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the information system.

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content and shall conduct penetration testing, building on the system owner vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

The **system administrator or ISSO** shall perform and document an analysis of the information system deliverables searching for obvious ways in which a user can violate the information system security policy. The system owner shall document the disposition of the obvious vulnerabilities and the documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the information system.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content and shall conduct penetration testing, building on the system owner vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

VA-1(1) Vulnerability Analysis

The system owner shall document the disposition of identified vulnerabilities. The documentation shall justify that the information system, with the identified vulnerabilities, is resistant to obvious penetration attacks.

The certifier, during the C&A process, shall perform an independent vulnerabilities analysis; shall perform independent penetration testing based on the independent vulnerability analysis to determine the exploitability of additional identified vulnerabilities in the intended environment; and shall determine that the information system is resistant to penetration attacks performed by an attacker possessing a low attack potential.

The **system administrator or ISSO** shall perform **and document an analysis of the information system deliverables searching for obvious ways in which a user can violate the information system security policy. The system owner shall document the disposition of the obvious vulnerabilities and the documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the information system.**

The certifier, during the C&A process, shall **confirm that the documentation provided meets all requirements for the content and shall conduct penetration testing, building on the system owner vulnerability analysis, to ensure obvious vulnerabilities have been addressed.**

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

VA-2 Examination of Guidance

The system owner shall provide guidance documentation. The guidance documentation shall identify all possible modes of operation of the information system (including operation following failure or operational error), their consequences and implications for maintaining secure operations. The guidance documentation shall be complete, clear, consistent, and reasonable; shall list all assumptions about the intended environment; and list all requirements for external security measures (including external procedural, physical and personnel controls).

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for content, shall repeat all configuration and installation procedures to confirm that the information system can be configured and used securely using only the supplied guidance documentation, and shall determine that the use of the guidance documentation allows all insecure states to be detected.

The **ISSO shall provide the ISSM with the complete Certification and Accreditation documentation suite.** The documentation shall identify all possible modes of operation of the information system (including operation following failure or operational error), their consequences and implications for maintaining secure operations. The documentation shall be complete, clear, consistent, and reasonable; shall list all assumptions about the intended environment; and list all requirements for external security measures (including external procedural, physical and personnel controls).

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for content, shall repeat all configuration and installation procedures to confirm that the information system can be configured and used securely using only the supplied guidance documentation, and shall determine that the use of the guidance documentation allows all insecure states to be detected.

VA-2(1) Examination of Guidance

The system owner shall document an analysis of the guidance documentation that demonstrates the guidance documentation is complete.

The certifier, during the C&A process, shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the information system.

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

The **ISSO shall provide the ISSM** with a gap analysis **and POA&M list (if required) that demonstrates the C&A** documentation is complete **and ready for the DAA to review.**

The certifier, during the C&A process, shall confirm that the analysis documentation shows that secure operation in all modes of operation of the information system is provided.

***MA-3(1) Maintenance Tools**

The organization must define a process to approve, control, and monitor the use of information system maintenance tools and maintains the tools on an ongoing basis within the controlled area. The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.

***MA-4(3) Remote Maintenance**

The organization must define a process to authorize, monitor, and control any remotely executed maintenance and diagnostic activities, if employed. The organization does not allow remote maintenance or diagnostic services to be performed by a provider that does not implement for its own information system, a level of security at least as high as that implemented on the system being serviced, unless the component being serviced is removed from the information system and sanitized (with regard to organizational information) before the service begins and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system.

***MP-6(1) Media Sanitization & Disposal**

The organization must define a process to purge information system media, both digital and non-digital, prior to disposal or release for reuse. The organization tracks, documents, and verifies media sanitization and disposal actions. Tracking is for Accountable media. See DOE 470.4-4 chapter II.4.

***PE-18(1) Location of Information System Components**

The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. The organization plans the location or site of the facility where the information system resides with regard to

physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

***PE-4 Access Control for Transmission Medium**

The organization controls physical access to information system distribution and transmission lines within organizational facilities in accordance with 205.1-3.

IA-3 Verification of Secrets

The information system security controls shall provide a mechanism to verify that secrets meet at least two-factor strong authentication mechanisms prior to granting access to systems and the information and resources managed by that system.

The information system security controls shall provide a mechanism to verify that secrets meet at least two-factor strong authentication mechanisms prior to granting access to systems and the information and resources managed by that system. **Two-factor authentication must consist of (2 of 3) something you know, something you have or something you are. For stand-alone systems "something you have" is the drive itself.**

IA-5 Multiple Authentication Mechanisms

The information system security controls may provide passwords; fingerprints; smart cards or other nationally recognized approved mechanism to support user authentication. Information system security controls shall authenticate any user's claimed identity according to the [list the rules describing how the multiple authentication mechanisms provide authentication (e.g., the user must provide both a valid password and a fingerprint associated with the user identifier; or the user must provide a password and a smart card assigned to the user identifier)].

The information system security controls may provide passwords; fingerprints; smart cards or other nationally recognized approved mechanism to support user authentication. **For systems not connected to a network, the information system security controls for two factor authentication will include physical access control to the safe which contains the disk of classified information. Multi factor authentication will consist of "access to the limited area", knowledge of the safe combination, and logon ID/password to the system. For networked systems, two-**

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

factor shall include something you have (e.g., a token or fingerprint) combined with something you know (e.g., password).

AU-1 Security Alarms

The information system security controls shall include or exclude auditable events from the set of audited events based on the user identity and role and shall automatically alert the Information System Security Officer (ISSO) and/or the System Administration and take automatically lock out the system/user, or isolate the system/user upon detection of a potential security violation.

The information system security controls shall include or exclude auditable events from the set of audited events based on the user identity and role and shall automatically alert the Information System Security Officer (ISSO) and/or the System Administration and take automatically lock out the system/user, or isolate the system/user upon detection of a potential security violation. **Notification is through lockout and audit log entry for systems not connected to a network with alerting capability.**

AU-4(1) Profile Based Anomaly Detection

The information system shall employ automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. The information system shall employ automated mechanisms to alert security personnel of [list of additional inappropriate or unusual activities that are to result in alerts (e.g., Excessive login attempts across network; Access to privilege system files, Exceeding data quotas/transfers, Creation of account; Privileged account logged into multiple servers/ devices/applications; Attempts to access unauthorized sites/computers/devices/objects; Unauthorized shutdown/restart of system/device/application; Permission change for user/file/application; Use of privileged commands; and Unauthorized export from system to media)].

The information system shall **have the ability to centralize the analysis of the logs and employ software filters to do the first level sorts/analysis.** The information system shall employ automated mechanisms **(e.g. writing to audit log file, issuing alarms to a network console)** to alert security personnel of excessive login attempts across network; access to privilege system files, exceeding data quotas/transfers, creation of account; privileged account logged into multiple servers/ devices/applications; attempts

to access unauthorized sites/computers/devices/objects; unauthorized shutdown/restart of system/device/application; permission change for user/file/application; use of privileged commands; and unauthorized export from system to media).

EN-8 Intrusion Detection

The site and network (when applicable) environment shall provide the ability to detect (i.e., using methods readily available on the Internet to attack known vulnerabilities) and sophisticated attacks on the network, network components, and hosts from inside or outside the site, including measures to detect and respond to unauthorized attempts to penetrate or deny use.

The site and network (when applicable) environment shall provide the ability to detect (i.e., using methods readily available on the Internet to attack known vulnerabilities) and sophisticated attacks on the network, network components, and hosts from inside or outside the site, including measures to detect and respond to unauthorized attempts to penetrate or deny use. **For systems that are not networked, audit logs and physical access records may be acceptable compensatory controls.**

EN-9 Information System Interface

The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external connection, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted. The information system denies information flow by default and allows information flow by exception (i.e., deny all, permit by exception). The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

The information system **must have perimeter protection that implements a managed interface with any external connection, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.** The information system denies information flow by default and allows information flow by exception (i.e., deny all, permit by exception). The organization

prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

PT-2 Information System Security Control Data Transmission

The information system security controls shall protect all information system security control data transmitted from the information system to a remote trusted IT product from unauthorized disclosure during transmission.

The information system **protects the integrity of transmitted information. The organization employs cryptographic mechanisms in accordance with DOE 205.3-1 to recognize changes to information during transmission unless otherwise protected by alternative physical measures. The information system must incorporate an NSA-approved secure tunneling protocol capability between systems to protect information from unauthorized disclosure during transmission.**

TP-1 Trusted Path

The information system security controls shall provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure. The information system security controls shall require the use of the trusted path for initial user authentication and [other services for which trusted path is required (e.g., transmission authorizations, authentication to resources, etc.)] and shall permit the information system security controls, local users, or remote users to initiate communication via the trusted path.

The information system **must incorporate a distinct NSA-approved secure device between communication paths to protect information from unauthorized disclosure during transmission.**

CO-2 Proof of Receipt

The information system security controls shall be able to generate evidence of receipt for received [list of information types (e.g., Confidential/Secret, Secret RD, Confidential RD, Secret RD 1-13, etc)] at the request of the originator, recipient, ISSO, or [list of third parties (e.g., system owner, ISSM, project management, etc.)] and provide a capability to verify the evidence of origin

of information to the originator, recipient, or [list of third parties (e.g., system owner, project management, etc.)] given [limitations on the evidence of origin (e.g., access authorization, formal access authorization, need-to-know, etc.)]. The information system security controls shall be able to relate the [list of attributes (e.g., user ID, authorized, labels authorized, permission attributes))] of the recipient of the information, and the [list of information fields (e.g., header information, IP addresses, etc.)] of the information to which the evidence applies.

The system must be able to support third party digital signature exchange. The information system security controls shall be able to generate evidence of receipt for received [list of information types (e.g., Confidential/Secret, Secret RD, Confidential RD, Secret RD 1-13, etc)] at the request of the originator, recipient, ISSO, or [list of third parties (e.g., system owner, ISSM, project management, etc.)] and provide a capability to verify the evidence of origin of information to the originator, recipient, or [list of third parties (e.g., system owner, project management, etc.)] given [limitations on the evidence of origin (e.g., access authorization, formal access authorization, need-to-know, etc.)]. The information system security controls shall be able to relate the [list of attributes (e.g., user ID, authorized, labels authorized, permission attributes))] of the recipient of the information, and the [list of information fields (e.g., header information, IP addresses, etc.)] of the information to which the evidence applies.

DP-5 Export of User Data with Security Attributes

The information system security controls shall enforce the Mandatory Access Control (MAC) security policy when exporting labeled user data, controlled under the MAC security policy when exporting, outside the control of the information system by exporting the user data with the user data's associated security attributes. The information system security controls shall ensure that the security attributes, when exported outside the control of the information system, are unambiguously associated with the exported user data and shall enforce the following rules when user data is exported from the control of the information system:

- *When data is exported in a human-readable or printable form the authorized administrator shall be able to specify the printable label that is assigned to the sensitivity label associated with the data; each print job shall be marked in accordance with DOE CMPC requirements.*
- *When data is exported on removable media, the media must be marked and protected in accordance with DOE CPMC requirements.*
- *Devices used to export data with security attributes cannot be used to export data without security attributes unless the change in device state is performed manually and is auditable.*

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON

• *Devices used to export data with security attributes shall completely and unambiguously associate the security attributes with the corresponding data.*

The classification of the data must be displayed on the media when printed out. The information system security controls shall ensure that the security attributes, when exported outside the control of the information system, are unambiguously associated with the exported user data and shall enforce the following rules when user data is exported from the control of the information system:

• When data is exported in a human-readable or printable form the authorized administrator shall be able to specify the printable label that is assigned to the sensitivity label associated with the data; each print job shall be marked in accordance with DOE CMPC requirements.

• When data is exported on removable media, the media must be marked and protected in accordance with DOE CPMC requirements.

• Devices used to export data with security attributes cannot be used to export data without security attributes unless the change in device state is performed manually and is auditable.

• Devices used to export data with security attributes shall completely and unambiguously associate the security attributes with the corresponding data.

DV-1(1) Correspond. Demonstration

The HLD shall describe the purpose and method of use of all interfaces to the subsystems of the information system security controls, providing details of effects, exceptions, and error messages, as appropriate and shall describe the separation of the information system into security control-enforcing components and other subsystems.

For custom developed (not COTS) software, the High-level Description (HLD) shall describe the purpose and method of use of all interfaces to the subsystems of the information system security controls, providing details of effects, exceptions, and error messages, as appropriate and shall describe the separation of the information system into security control-enforcing components and other subsystems.

DV-2 Implementation of the information System Controls

The system owner shall provide the implementation representation for a selected subset of the information system security controls. The implementation representation shall unambiguously

define the information system security controls to a level of detail such that the information system security controls can be generated without further design decisions. The implementation representation shall be internally consistent.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content and presentation of evidence and determine that the least abstract information system security controls representation provided is an accurate and complete instantiation of the information system security functional requirements.

The **software developer** shall provide the implementation representation for a selected subset of the information system security controls. The implementation representation shall unambiguously define the information system security controls to a level of detail such that the information system security controls can be generated without further design decisions. The implementation representation shall be internally consistent.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content and presentation of evidence and determine that the least abstract information system security controls representation provided is an accurate and complete instantiation of the information system security functional requirements.

DV-3 Information System Security Policy Model

The system owner shall provide an information system security policy model. The system owner shall demonstrate correspondence between the functional specification and the information system security policy model. The information system security policy model shall describe the rules and characteristics of all policies of the information system security policy that can be modeled and include a rationale that demonstrates that it is consistent and complete with respect to all policies of the information system security policy that can be modeled. The demonstration of correspondence between the information system security policy model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the information system security policy model.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

The **software developer** shall provide an information system security policy model. The software developer shall demonstrate correspondence between the functional specification and the information system security policy model. The information system

security policy model shall describe the rules and characteristics of all policies of the information system security policy that can be modeled and include a rationale that demonstrates that it is consistent and complete with respect to all policies of the information system security policy that can be modeled. The demonstration of correspondence between the information system security policy model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the information system security policy model.

The certifier, during the C&A process, shall confirm that the documentation provided meets all requirements for the content.

***PE-6(2) Monitoring Physical Access**

The organization monitors physical access to the information system to detect and respond to physical security incidents. The organization employs automated mechanisms (cameras, access controlled doors) to recognize potential intrusions and initiate appropriate response actions

***PE-8(2) Access Records**

The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records [Assignment: organization-defined frequency]. The organization maintains a record of all physical access, both visitor and authorized individuals.

***SA-5(2)Information System Documentation**

The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

APPENDIX XIII: NSS MANUAL CONTROL COMPARISON